

Vision Version 4.1



VingCard, VingCard Vision and Da Vinci by VingCard are registered trademarks of VingCard A.S

Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such.

CHAPTER 1 : INSTALLATION	4
OVERVIEW OF INSTALLATION	4
INSTALLING THE NETWORK	5
INSTALLING VINGCARD VISION	6
SETTING AND CHECKING ACCESS RIGHTS AND USER PERMISSIONS	11
INSTALLING MICROSOFT ACTIVESYNC.	15
ENABLING AUTOMATIC LOGON IN WINDOWS NT / 2000 / XP.	15
SET UP VISION SUB-NETWORKS USING VC_NET.INI	16
UNINSTALLING VINGCARD VISION	17
CHAPTER 2 : SYSTEM OVERVIEW.....	18
WHAT'S NEW IN VISION 4.1	18
VC 3000 vs. VISION TERMINOLOGY	19
SYSTEM COMPONENTS	20
BASIC SYSTEM OPERATIONS	28
SYSTEM CONFIGURATION EXAMPLES	34
THE VISION LICENSING AGREEMENT	35
CHAPTER 3 : PLANNING THE SYSTEM.....	38
OVERVIEW OF SYSTEM PLANNING.....	38
WORKSHEET EXAMPLES	39
BLANK WORKSHEET FORMS.....	55
CHAPTER 4 : USING LOCKLINK.....	61
LOCKLINK OVERVIEW	61
INSTALLING THE VISION LOCKLINK SOFTWARE.....	63
LOADING LOCK DATA FROM VISION WORKSTATION	80
STARTING THE LOCKLINK	83
LOCKLINK FUNCTIONS	85
CHAPTER 5 : USING VISION MODULES.....	99
HOW TO EXIT THE VISION SYSTEM.....	99
MAIN MENU OF VISION MODULES	100
SYSTEM SETUP MODULE	103
GUEST KEYCARDS MODULE.....	190
EMPLOYEE KEYCARDS MODULE	211
EMPLOYEE ROOMS MODULE	229
SPECIAL KEYCARDS MODULE	246
SYSTEM USERS MODULE	266
BACKUP MODULE.....	275
LOCKLINK MODULE	280
REPORTS MODULE.....	286
GLOSSARY OF TERMS	299
FREQUENTLY ASKED QUESTIONS	300
CHAPTER 6 : PMS INTERFACE.....	302
ABOUT INTERFACING VISION WITH A PMS	302
HOW TO USE THE PMS SYSTEM	302
WHERE TO FIND DETAILED INFORMATION ON THE VISION PMS INTERFACES	302
SPECIFIC PMS ISSUES IN 'MIXED CARD' PROPERTIES	302
CHAPTER 7 : NETWORK ENCODER SETUP.....	304
GAREK NETWORK ENCODERS	320
KDE SERIES 493X NETWORK ENCODERS	304
NETWORKING XAC SMART CARD ENCODERS	319

CHAPTER 8 : BATCH MODE	332
INTRODUCTION	332
INSTALLATION	332
SYSTEM OVERVIEW	333
COMMUNICATION	334
OPERATION OF THE VISION SYSTEM IN BATCH MODE	335
CHAPTER 9 : IMPORT EXPORT.....	341
INTRODUCTION	341
GENERAL INFORMATION	341
CHAPTER 10 : USING NBS ENCODERS	346
INTRODUCTION	346
HOW TO SET UP A VISION SYSTEM TO USE NBS ENCODERS.....	347
HOW TO SET UP NBS ENCODERS FOR USE WITH VISION	349

Chapter 1 : Installation

Overview of Installation

VingCard Vision can be installed on a single PC or on a system with several PCs connected together in a network. Vision can either use a dedicated network, or work over an existing network at the installation property.

In a networked system, all workstations use the same database. The PC that runs the database is referred to as the VingCard server. All other PCs are referred to as workstations. Each PC has access to its own locally connected devices and also to all of the networked encoders and printers.

Each PC in the network must have a unique identification. Those identifications are the computer names as seen from the network. The computer names used by VingCard Vision are STATION_000, STATION_001, and so on up to STATION_099. The PC set up as the server is by default STATION_000, although the Vision installation program allows any computer to be set up as the server.

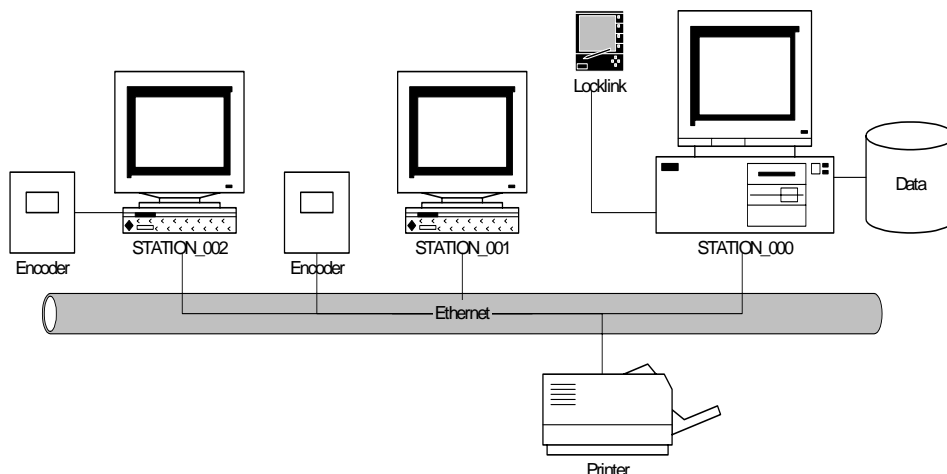


Figure 1.

It is recommended that installation of VingCard Vision is carried out in the following order :

- Install and configure the network, first on the server then on each workstation.
- Install VingCard Vision first on the server then on each workstation.
- Set and Check network access rights and user permissions
- Install Microsoft ActiveSync on any PCs that will communicate with LockLink
- Enable automatic network logon if required (Windows NT / 2000 / XP only)
- Set up Vision sub-networks using vc_net.ini - if required (for example where two hotels, each with their own Vision installation share a common corporate network)

Installing the Network

STEP 1: Selection of network PCs and Operating Systems.

VingCard Vision can run under the following operating systems (OS): Windows 98, Windows NT (4.0 or later), Windows 2000, Windows XP.

If possible, the VingCard Server in networked systems should use one of the more stable operating systems (NT, 2000 or XP).

STEP 2. Cabling

Connect all workstations with the type of cabling required by your network cards.

STEP 3: Install cards.

If you are using VingCard Vision Workstations (see picture) go to Step 3.



If you have only one PC in your system, go to Step 3.

Otherwise, carry out this step, first on the server, then on each workstation.

If the PC does not have a network card installed, obtain a network card compatible with Microsoft Network peer-to-peer connections and install it according to the vendor's instructions. Normally this involves opening the computer enclosure and installing the card in a free slot, or insertion of a PCMCIA network card in a PCMCIA slot. Restart the PC and let Windows configure itself automatically (Plug And Play). If Windows is not able to do this automatically, check the documentation for your network card. You will probably have to use the Add New Hardware wizard from within Control Panel.

Important note : If you are using network hubs to link one or more PCs in the Vision network, check that the Duplex settings for your network cards are compatible with those for your hubs. Mismatches here can cause very slow performance. The Duplex settings (if present for your adaptor) can be found under:

Start /Settings/Control Panel/Network/Adaptors/Configure/Advanced.

STEP 4: Configure network protocols.

Carry out this step first on the server, then on each workstation.

Each PC running Vision needs

- TCP/IP protocol installed
- File and Printer Sharing for Microsoft Networks enabled
- A unique computer name set. You can either use STATION_000 etc, another naming convention or simply the existing computer names set up on an existing network.
- A unique IP address. You can either allocate these yourself or allow the network to set them (via DHCP). In either case, all IP addresses must be on the same subnet IP addresses can be found by typing IPCONFIG at the command prompt.

If one or more IPX/SPX protocols are installed, then remove them if you are sure they are not needed. They are not needed in a Vision only system. You must NOT remove them if you will be installing VingCard Vision on a system already using Netware

Windows must be restarted before any changes you make to network / TCP/IP settings take effect. Select **Yes** if Windows asks if you want to restart your computer.

Installing VingCard Vision

You will need your installation CD and License codes (delivered with Vision).

STEP 1 Run the Version 4.1 installation program, V41Install.exe

Carry out this step, first on the server, then on each workstation. For PCs already set up with different levels of Windows user, make sure you log on with Administrator rights before running the install program.

Follow the instructions presented by the installation program and select appropriate options.

NOTE 1: Upgrading old Vision installations

- **Pre Version 3.1 installations**
When installing on a server with an existing Version 2, Version 3.0 or Version 3.01 Vision installation, you must first convert to Version 3.1. First make a backup of the existing (v2, 3.0 or 3.01) database, then run the Vision 3.1 installation program V31Install.exe, selecting 'Keep Database' when prompted. You do not need to install any V3.1 Service Releases.

Once your database is at Version 3.1, the Version 4.1 installation program can automatically convert it.

- **Version 3.1 and version 4.0 installations**
When your Vision installation is at Version 3.1 or 4.0, you can upgrade directly to Version 4.1. Select 'Keep Database' when prompted and the Version 3.1/4.0 database will be upgraded in line with Vision 4.1 requirements. It is strongly recommended that a backup of the old database is taken before installation of V4.1.

Note that the installation path that you select for Vision 4.1 should not contain any space characters. Example: "C:\Vision_41": OK ; "C:\Vision 41": not OK.

After selecting 'Keep Database' you will be prompted to select a default Lock Type (for example 'VC3000 Classic' or 'Presidio Combo'). If your property uses more than one of the lock types listed, you should select the most common lock type as a default and then, after installation is complete, use **Vision > Setup > Locks > Lock Groups > Change Existing** in order to allocate the other lock types to the relevant doors.

You will then be asked to select a default Card Family, either **mag-stripe**, **memory card** or **smartcard**. You should select the type of keycard that your property will predominantly use. If your property will use more than one of the card family types listed, you should select the most common type as a default (normally but not always mag-stripe) and then, after installation is complete, use **Vision > Setup > User Groups > Change Existing** in order to allocate the other card families to the relevant user groups.

smartcard : a card which uses a memory chip to store information and additionally has built in processing power.

memory card : a card which uses a memory chip to store information but has no built in processing power.

Note that VingCard dual reader ('Combo') locks can read mag-stripes, memory cards and smart cards. User groups that need access to these locks should be assigned either the mag-stripe or the smartcard card families.

There are a small number of Vision locks (Marketed as 'VC3000 Smart Card') that can only read memory cards – not smartcards. The only time a user group should ever be allocated the 'memory card' card family is when the property is equipped with these locks and mag-stripe access is not desired.

- **Changing a previous server to a workstation**
When installing on a workstation that was previously a server, any old version 3.x databases found are deleted.
- **DaVinci installations**
DaVinci databases are NOT automatically converted by Vision installation.

NOTE 2: When prompted for the installation type

For the server, select the appropriate type:

- **Peer Server:** the server will contain the database and the VingCard Vision program.
- **Database server:** the server will contain the database only. In this case, Vision cannot be run on the server, only remotely via workstations.
- **Workstation:** the Vision program will be installed, configured to access the database on the Vision Server.

NOTE 3: When installing on a Workstation

In order that Vision can access the data base on the Vision Server you will be prompted to enter the name of the Vision Server PC. If upgrading from Vision 3.x, the entry will default to the Vision Server name previously used. For new installations, you must know and type the Computer Name of the Vision Server PC. The method of viewing or changing a Computer Name is operating system dependant. Refer to Windows help from the start menu and look up 'Computer Name'.

NOTE 4: Installing a 'Construction' database

The initial installation (construction) at a Hotel can be done with a pre-programmed 'construction' facility code and can be based on simple pre-made database, sufficient for use at the construction stage.

The construction database can be selected (as an alternative to 'Demo' or 'Empty') from the Vision installation program. When Vision is operating with a Construction database, indication is given on the Log In Screen. You will not need to enter any License codes. These will be delivered at a later date – at which point Vision must be re-installed using them.

All the locks can initially be programmed with CONSTRUCTION facility code and data according to construction database. Then when VingCard provides the final facility code and final database is set-up, you can OVERWRITE the locks with new data (including facility code), without the necessity to disconnect a battery for clearing RAM in lock.

To utilize the Construction OVERWRITE functionality you must check the construction lock check box on the system tab of LockLink.

When the check box is unchecked, LockLink operates in the normal way - the Facility Code from the database is loaded into the locks – provided the locks do not contain another facility code.

When the check box is checked, locks with the Construction Facility Code will be updated with the new Facility Code (the one newly uploaded from Vision to locklink).

NOTE 5: When prompted to select between standard and batch mode

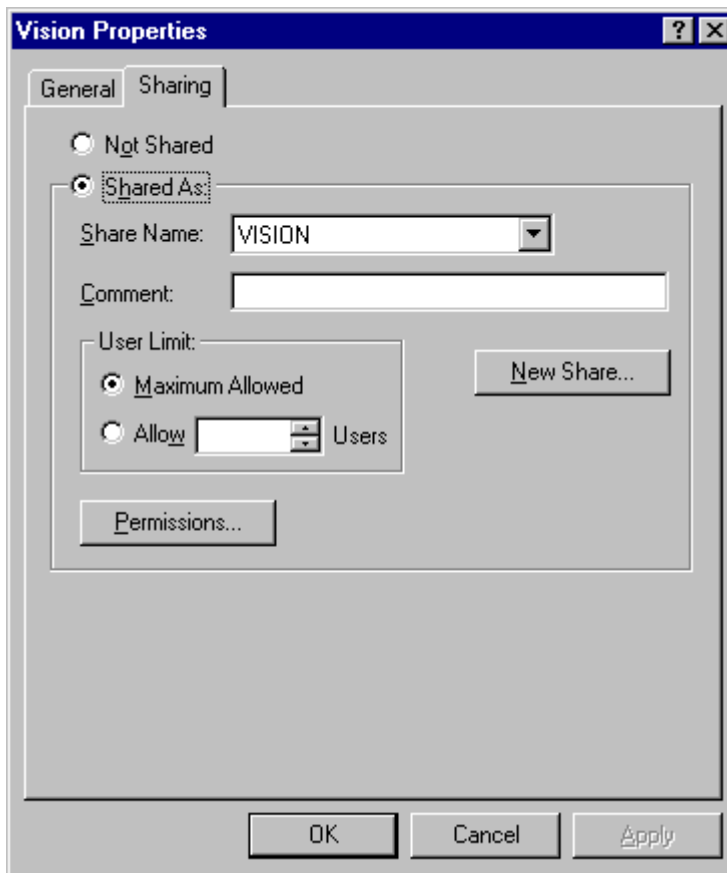
Batch mode is a specialist mode of operation where Vision creates output files that are read by third party software in order to make keycards on batch encoder / printers. Some cruise line companies use batch mode. Only select batch mode installation if you are installing at one of these installations, otherwise, select 'standard' (the default).

Further details of batch mode are available in Chapter 8 of the Vision Manual.

STEP 2. Make 'Vision' folder available by Sharing (Windows 98)

Carry out this step on the **Server only**. Note: For Windows 2000, NT or XP servers, the installation program will carry out this step for you.

Double click **My Computer** on the desktop. Right-click on the icon for the folder where Vision is installed. Click **Sharing**. Click **Shared as:** and fill in **Share name:** for your shared folder. The name must be **VISION**. (The **Comment:** field is optional.) Set **Sharing permission** to **Full control**. If you encounter problems while setting up Sharing, see 'Sharing folders' in Windows Help. The window should now look similar to this (example is from Windows NT):



Click **OK**. Note that the icon for the Vision folder has changed.

STEP 3. Make local printers available over the network

Carry out this step on all stations that are directly connected (serial or parallel cable) to a printer that you want to be shared by other Vision stations.

Install the printer to the local PC. Go to the Windows printer folder (**Start button > Settings > Printers**). Right-click the printer you want to share and then click **Sharing**. Select **Shared as:** and fill in **Share name:** for your shared printer. The name can be **HewlettPackard 400**, for example. (The **Comment:** field is optional.) Click **OK** and the printer's icon will be changed.



Shared drive



Printer folder



Shared printer

STEP 4. Set up a default printer for each Vision station

Carry out this step on all stations that you wish to view, save or print Vision reports from.

Go to the Windows printer folder (**Start button > Settings > Printers**). Consider the printer that you want to be the default for the particular Vision station. If it is not listed, use the **Add Printer** option to add it. Select the printer from the list of those available and set it as default (Select from list, right click, **Set as default**).

STEP 5. Hiding the taskbar

This step is optional. If desired, carry out this step, first on the server, then on each workstation.

The taskbar (normally at the bottom of the screen) can be hidden clicking **Start button/Settings/Taskbar**. Then check the **Auto Hide** box and click **OK**.

STEP 5. Autostart of VingCard Vision.

This step is optional. If desired, carry out this step first on the server, then on each workstation.

After successful installation of a peer server or server, the Vision database server will start each time Windows is started.

If you want the Vision program to start automatically when Windows is started, you need to prepare this manually. To do this click **Start button/Settings/Taskbar** and then click the **Start** menu, **Programs** tab. Click the **Add** button. In the **Command line:** field now type **c:\vision\vision.exe** (or use a different path if you installed to a folder other than c:\vision). Click the **Next** button and now double-click the **StartUp folder**. In the field **Select a name for the shortcut:** type **VingCard Vision** and then click the **Finish** button. Click **OK**.

Setting and Checking Access Rights and User permissions

Background

Access rights and user permission issues are becoming increasingly significant to the operation of networked Vision installations as windows networks continue to migrate towards NT/2000/XP solutions.

The most relevant issues are

- **Folder sharing and associated permissions**
Can prevent access to server files if incorrectly set. Sharing and sharing permissions are relevant to all Windows versions. For Windows NT and later, sharing is correctly set during Vision installation. However, it might be incorrectly changed later. For Windows 98, sharing must be set up manually as described previously.
- **Registry Permissions**
Can prevent Vision from retrieving and using important path information if incorrectly set. Registry permission is only relevant to Windows NT and later and is correctly set during Vision installation. However, it can be incorrectly changed later.
- **Network User accounts and permissions**
Can prevent access to server files if incorrectly set and also problems with time synchronisation. For multi-user systems, suitable users for operating Vision must be set up manually.

Indications of User permission problems

User permission problems can show themselves in the following ways in a VingCard Vision system

Unable To Store Facility Code Message

When starting Vision, a message is displayed: "Unable to store facility code. Check that..." Vision continues to partially operate, but certain functionality is unavailable. For example, attempts to make a Guest key will provoke the message "License limit exceeded"

This problem can be caused by problems with

- Folder Sharing
- Registry Permissions
- Network User Accounts and Permissions

Vision Locklink module cannot access lock files

From a workstation, when you select the Vision Locklink module a message is displayed 'File Not Found'. When you press 'OK' a more detailed error message appears in red text in the 'Status' panel.

This problem can be caused by problems with

- Folder Sharing

- Registry Permissions
- Network User Accounts and Permissions

Vision does not complete a backup

The error message 'Error: did not complete the backup!!!' is received when attempting to make a backup or when running an autobackup. Either the backup path cannot be determined from the registry (due to insufficient registry permission) or the specified path can be determined but not written to by the currently logged on user.

This problem can be caused by problems with

- Folder Sharing
- Registry Permissions
- Network User Accounts and Permissions

Workstation does not act on Time Synch message

A vision station (usually the server) issues a time synch command as determined by set up settings but one or more other stations do not synchronize their time.

This problem can be caused by problems with

- Network User Accounts and Permissions

How To Set Up User Permissions For Vision

Folder Sharing

The main Vision folder on the Vision server must be shared.

For Windows NT, 2000 & XP, the share is automatically made during installation.

For Windows 98 sharing has to be set manually. The process for this is described at step 2 of the 'Installing VingCard Vision' instructions.

You can check the share on the Vision server by using Windows explorer / My Computer, selecting the main Vision folder, right clicking, selecting **Sharing** and observing the share properties. They should be as outlined at Step 2 of the 'Installing VingCard Vision' instructions. If they are not, change them.

Registry Permissions

This is relevant to any PC on the Vision network running **Windows NT, 2000 or XP**.

Vision automatically sets the correct registry permissions during installation - but it is important that you were logged on with an administrator password during installation.

You can check and change these settings at the Vision server and at each workstation as follows:

The following steps assume that all Vision users belongs to the group "Everyone".

- Logon to the PC with Administrator access rights.
- Select Start > Run.

- Type regedt32.exe + <enter> to run the 32 bit Registry Editor.
- Select "HKEY_LOCAL_MACHINE"
- In the registry key tree, open the "SOFTWARE" key.
- Locate and highlight the "Vingcard" subkey.
- Select the menu option Security/Permissions...
- Check the option "Replace Permission on Existing Subkeys"
- Verify that the group "Everyone" is listed in the member group listbox. If not, press ADD and add it to the list.
- Double-click the group "Everyone".
- Check the "Full control" radio-button and press OK.
- Press OK and select "Yes" to the question to confirm the changes.
- Exit the Registry Editor.

Repeat the process for each affected NT, 2000, XP PC running Vision SW.

Network User Accounts and Permissions

This is relevant to any workstation on a Vision network **where the server is either Windows NT, 2000 or XP.**

Access to the server

Log on to each workstation using a typical user account for staff that will use Vision. Use Network neighborhood (or equivalent) to locate the server machine. Highlight and double click. If you gain access to the machine, then network permission is not a problem; if you are prompted for a user name and/or password, it may be. In order for Vision to work you need to log on to the server from the workstation.

If this is the problem, the best way to solve it permanently is to create compatible user accounts (same username and password) on the server and workstation PCs. In this way, the username and password that you type to log on to the workstation is also used to gain access to the server with no additional input required.

There are two basic ways to tackle this:

- Set up one account on the server, an equivalent account (same user and password) on each workstation and always log into each workstation with that account when using Vision.
- Set up multiple accounts on each workstation (in line with the property's policy) and mirror each on the Vision server.

Simple example: put the server and all workstations on a common workgroup (such as 'VingCard'). Create a user 'Vision' on the server and assign a password. Now create user accounts with the name 'Vision' and the same password on all workstations. Log on to workstations using the 'Vision' accounts. You can also log onto the server with the 'Vision' account but it is not essential. The important thing is that the server receives any valid username/password combination from the workstation.

For more complex networks, possibly involving domain servers etc. things may be more complex. However, the basic theory is the same: try to find or set up a workstation account that automatically provides access to the shared Vision folder on the server. The final solution chosen must take account of other User / traceability issues relevant to the property where the Vision network is installed.

Note that on Windows 98 PCs, you may want to activate multiple users (in order to automatically supply a username and password to the Vision server). You can do this via Control Panel > Passwords > User Profiles, check the 'All users can customize....' Tab. When you restart, use the new username and password to login. This will create the new user.

Note also that with a Windows XP server, if you set up a user without a password (which is allowed) and then try and log on and connect through Win 98/NT/2000 workstations using the same username but leaving the password blank, you will not be connected. Therefore, it is necessary to define and use a non-blank password.

Local Rights necessary in order for Time Synch to work

For the Vision time synchronization function to work each workstation running vision must be logged in with sufficient user rights to allow the date / time to be modified.

You can check this for each relevant user. If you can't change date / time via Control Panel, then Vision will not be able to change it either. You must then increase User Rights.

Under Windows 2000, Standard User will work, Restricted User will not.

Under Windows NT, Power User will work, User will not.

Avoid Windows password (Windows 98 only).

For Windows 98 the very first time you start up Windows you might be asked to enter a password for Windows (as opposed to the network). VingCard Vision is protected by its own password system, therefore a Windows password is unnecessary.

To disable the windows password you must replace the existing password with an empty password. To do this click Start button/Settings/Control Panel/Password/Change Window Password. In this dialog, enter your existing password and leave the fields for New password and Confirm new password empty. Click OK.

Testing the Vision Network for Correct User Permissions

To test the Vision network for correct permissions.

- Log on to the server using the username and password that will normally be used. Start Vision.
- Log on to each workstation using a typical 'lowest permission' user at each.
- Start Vision at each PC and check that the 'Unable to store facility code....' Message is not displayed.
- Use setup to send a time synch message from the server to all workstations and check that they all act on it.
- Perform a backup from each workstation (or a representative selection) saving the backup files on the server machine.

If there is still a problem

If you have checked folder sharing, registry permissions and user access rights but you still suspect an access / permission problem you can also try the following :

Use server IP address instead of computer name

This can be tried on any operating system and for any version of Vision – but only where the server IP address is fixed (not dynamically allocated using DHCP).

At the workstation, Start > Run > Regedit.

Navigate to HKEY_LOCAL_MACHINE\Software\VingCard\Vision

Change VisionNetPath value from \\servername\vision format to \\IpAddress\Vision (for example \\172.16.30.100\Vision)

Installing Microsoft ActiveSync.

Any Vision PCs – server or workstations – that will be used to transfer data to and from the LockLink need Microsoft ActiveSync to be installed.

Microsoft ActiveSync is delivered along with VingCard LockLink units. Details of how to install it are given in Chapter 4 (LockLink) of this manual.

Enabling automatic logon in Windows NT / 2000 / XP.

Automatic logon allows users to avoid the network login after a PC is started. In effect, this may mean that they avoid having to remember a suitable Windows password that is different to their VISION password.

Automatic Logon may be needed for users who do not share computers and wish to quickly log onto a network. Automatic Logon may also be used for networks who have one default logon for their users.

Setting Automatic Logon Manually

To configure Windows NT / 2000 / XP to automatically login will require the registry to be edited and the following instructions to be carried out.

- Run Regedit32.exe
- Open the following key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon
- Within the above key enter the values normally entered into the following values:
DefaultDomainName
DefaultUserName
DefaultPassword
- If DefaultPassword is not present to create a new value click Edit, choose Add Value. In the Value Name field type DefaultPassword. Select REG_SZ for the Data Type. In the String field type your password and save changes.

- In addition if no DefaultPassword string is specified, Windows NT automatically changes the value of the AutoAdminLogon key from 1 to 0, thus disabling AutoAdminLogon feature.
- From the Edit menu, choose Add Value. Enter AutoAdminLogon in the Value Name field. Select REG_SZ for the Data Type, enter 1 in the string field and save your changes.
- Finally if DONTDISPLAYLASTUSERNAME value is set to 1, Autoadminlogon does not function.

To bypass the automatic logon in the future press and hold the SHIFT key as the computer is booting.

Setting Automatic Logon Automatically

It is also possible to set automatic logon using the Microsoft TweakUI program which can be installed into Control Panel. TweakUI is freely available on the internet and DOES work with all windows versions up to and including XP. Install TweakUI then use Help for instructions.

Automatic Logon Security Issues

For Windows 98/NT using auto logon can be a security risk, as the **DefaultPassword** is stored in plain text in the registry.

In Windows 2000, if you use the TweakUI program [TweakUI Logon](#) tab to set the registry entries, the **DefaultPassword** value name is **NOT** created at the **Winlogon** key. Instead, a <NO NAME> value name, using the **REG_DWORD** data type, is created at **HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets\DefaultPassword**. This data value is encrypted and **NOT** viewable.

In Windows XP the password is also encrypted if you use TweakUI, although not at the registry location mentioned for Win 2000.

Set up Vision sub-networks using vc_net.ini

If you have more than one Vision installation connected to the same corporate network, you may wish to isolate the installations from each other to guard against unwanted interaction. You can do this by editing the vc_net.ini file on each PC.

VC_NET is a program that runs in the background on all PCs where Vision is running. It handles network communication between Vision stations. The VC_NET program uses a simple, one-entry INI file, vc_net.ini in order to allow networked PCs to mask out broadcast messages. This file is used by the VC_NET program to create a 'virtual network'. VC_NET programs with a specific 'Site Value' will only receive messages from other VC_NET programs that have the same Value specified in this file. If this file does not exist, the default Site Value will be '1'.

The contents of a typical file VC_NET.INI are as follows :

[Site]
Value=1

Therefore, if a PC with Value=1 in its vc_net.ini file broadcasts a message, only other networked PCs that also have Value=1 in their own vc_net.ini files will act on the message. Different 'sub-networks' can therefore easily be created by setting 'Value' to other values. **This must be done on all PCs, not just the server.**

For example, when a command is sent from Restorer.exe to shutdown all Vision stations, only those with a matching value in VC_NET.INI will be shut down.

Uninstalling VingCard Vision

To uninstall VingCard Vision 4.1:

Select **Start > Settings > Control Panel > Add/Remove Programs**.

Select **Vision** from the list of installed software, and click **Change/Remove**.

Follow the instructions in the Uninstall program to uninstall VingCard Vision 4.1

Chapter 2 : System Overview

What's New in Vision 4.1

Vision 4.1 adds more functionality to the Vision product, creating the most feature-rich, flexible hotel keycard system on the market.

<p>Restricted passage mode — Passage Mode can be disabled for group of locks.</p>
<p>If lock-group has “Prevent Passage Mode” flag checked, then all locks, belonging to such group, will always stay in normal mode.</p>
<p>Batch card encoding in TCP/IP interface — Vision 4.1 can be set up to perform the batch encoding of guest or passenger cards over TCP/IP interface. Previously, this feature was available solely for RS-232 interface.</p>
<p>MACE interface — Vision 4.1 offers an interface for providers of 3rd party software to pass encoding information for mag-stripe tracks 1 and/or 2 – allowing Vision to encode fully customized information relating to individual customer needs - for example for safe access or car parking.</p> <p>Such software is named MACE – <u>M</u>ulti-<u>a</u>pplication <u>C</u>ard <u>E</u>ncoding. Usage of MACE is controlled by license codes.</p>
<p>Improved reading of magnetic cards — Lock programs, available with Vision 4.1, provide much better reading of magnetic stripe, which minimizes the number of red flashes for valid cards.</p>

VC 3000 vs. Vision Terminology

Many new Vision users are familiar with the terminology used in the VC 3000 system. The following table indicates the new terms for the following:

	VC 3000 Name	Vision Name
1	Access Point	Common Door
2	User Type	Keycard Type
3	MOC	Lift Controller/MOC
4	Guest Sections	Suite/Connected Rooms
5	Internal Mode Control	Lock Open Time Table
6	Room Type Guest Others	Lock Group Guest Door Locks Custom
7	Lock Type VingCard Customise	Lock Motor Type VingCard Custom
8	Country Code	Not necessary – Windows setting is used
9	CPU Keyboard Time-Out and Device Time-Out	Workstation Time-Out

System Components

The Door Locks

Vision 4.1 supports the full range of VingCard electronic locks : DaVinci, VC3000 Classic and Presidio.

General Lock Features

- When a guest occupies a room, their complete privacy is insured by extracting a deadbolt. The deadbolt can only be retracted from outside the room with the (metal) Emergency Key (for locks with cylinders), a keycard with authorized deadbolt override, or with the LockLink.
- Both the deadbolt and latch bolt can be retracted by use of a keycard authorized for deadbolt override. If no deadbolt override is assigned to the card, the indicator on the outside escutcheon, just above the card insertion slot, displays a yellow light when the card is inserted.
- The lock can always be opened by pressing the inside handle even if the deadbolt is extracted. This serves as an emergency exit.
- VC3000 Classic and DaVinci locks have an option for metal cylinders to be fitted. Presidio locks never have metal cylinders. On locks with a cylinder, a metal emergency key (EMK) key operates the cylinder and overrides the deadbolt. If the deadbolt is thrown, turn the key 360 degrees to retract the deadbolt, then turn an additional 120 degrees to retract the latch. Only a metal EMK key can extend a deadbolt from outside a room.
- A new guest card automatically locks out the keycard of the previous guest. This is accomplished by assigning a start time to the card. When the card is issued, the system writes the present time onto the card.
- All types of lock use standard AA batteries. Consult your local VingCard dealer for the best current advice regarding good quality batteries.

The DAVINCI lock



With a powerful processor and extensive memory capacity, the DAVINCI lock is capable of managing information from both mag-stripe and Smart Cards simultaneously. This allows you to maximize the operational benefits of both technologies and provides for seamless system upgrades in the future.

DAVINCI's all-brass escutcheon features a uniquely designed upsert reader that provides user-friendly operation, as well as unparalleled protection from dust, moisture and tampering. A soft but highly visible LED communicates lock operation and status to the user. With surface mounted electronics for easier installation and maintenance, the DAVINCI lockset also meets the most stringent physical security and fire requirements.

Features

- Sleek contemporary design
- Ergonomic upsert reader
- Dual magstripe and smart card access control
- Simple, reliable magnetic and/or smart card reader
- High security lockset with a full 1" steel deadbolt, 3/4" anti-pick latch for added strength and 2 piece anti-friction latch
- High quality steel reinforced construction with solid brass handles
- Self lubrication long life bearings tested to withstand over 1.2 million openings without visible sign of wear
- Full mortise ANSI and EURO lock case options
- Modular components for design flexibility and easy maintenance
- "Panic release" - deadbolt and latch are automatically retracted by inside lever handle
- UL-fire rated

- Powerful "Flash" Memory Technology allows the lock to be easily reprogrammed and upgraded on site without replacing expensive hardware or components
- Automatic daylight saving adjustment
- 200 event audit trail stored in the lock
- Sealed electronics located on the inside of the door, enhance security and durability
- Unique emergency Recodable Cylinder option for mechanical override
- Cylinder tamper alarm as well as cylinder concealing option
- Standard AA-battery-operated, stand-alone locks require no wiring

Indications

A green/red/yellow LED indicates the following:

Function	LED
Low battery warning	3 yellow flashes
Guest privacy	1 yellow flash
Access granted	1 green flash
Lock-out card accepted	1 green flash
Undo lock-out card accepted	3 green flashes
Misread/wrong card	1 red flash
Scheduled Access mode – open	1 green flash each second
Lock communication OK	1 green flash
LockLink error	1 red flash
Command card accepted	1 green flash
Battery connected, application program installed	1 yellow flash when program is installed
Battery connected, application program not installed	1 yellow flash when battery is connected
Cylinder tamper alarm active	1 red flash each second

The VC3000 Classic lock



VingCard VC3000 Classic electronic locks have been carefully designed and engineered to our own exacting standards, in order to provide the quality you need to secure your valuable property and guests. Operated with a highly reliable magnetic stripe keycard system, the VingCard Classic lock offers a number of unique safety and operational features, yet they are exceptionally easy to operate and maintain. With over 15 years of proven performance in thousands of hotels throughout the world, VingCard Classic electronic locks continue to set the standards in the industry.

Features

- High security lockset with a full 1" steel deadbolt, 3/4" anti-pick latch for added strength and 2 piece anti-friction latch
- High quality steel reinforced construction with solid brass handles
- Self lubrication long life bearings tested to withstand over 1.2 million openings without visible sign of wear
- Full mortise ANSI and EURO lock case options
- Modular components for flexibility and easy maintenance
- "Panic release" - deadbolt and latch are automatically retracted by inside lever handle
- 3-hour UL fire rating
- Powerful "Flash" Memory Technology allows the lock to be easily reprogrammed and upgraded on site without replacing expensive hardware or components
- Up to 100 event audit trail stored in the lock
- Sealed electronics located on the inside of the door, enhance security and durability
- Unique emergency Recodable Cylinder option for mechanical override
- Standard AA-battery-operated, stand-alone locks require no wiring

-
- Simple, reliable magnetic stripe card reader. Keycards read during removal, for maximum performance

Indications

A green/red/yellow LED indicates the following:

Function	LED
low battery warning	3 yellow flashes
guest privacy	yellow
access granted	green
lock-out	1 green flash
undo lock-out	3 green flashes
misread/wrong card	red
internal control mode - open	green flash each 1 sec.
lock communication OK	green
LockLink error	red
command card accepted	green
Battery connected, application program installed	yellow + yellow
Battery connected, application program not installed	yellow

The Presidio lock



The Presidio lock combines VingCard's uncompromising standards of security, durability, quality and reliability with an attractively affordable price.

Features

- Standard magnetic card reader or optional 'combo' magnetic strip / smartcard reader. The dual reader works with both less expensive memory chip cards and/or more advanced processor cards.
- High security mortise lockcase available in ANSI or EURO versions. Presidio is constructed to ANSI grade 1 standards.
- Panic release – the deadbolt and latch are automatically retracted by inside handle for easy egress in emergencies.
- Handles and thumb turn in line with ADA (Americans with Disabilities Act) requirements.
- Modern composite material escutcheon provides superior corrosion resistance.
- Outside escutcheon is reinforced by a solid steel plate for extra security.
- Self lubricating long life bearings tested to withstand over 1 million openings without visible sign of wear
- Modular components for flexibility and easy maintenance
- Powerful "Flash" Memory Technology allows the lock to be easily reprogrammed and upgraded on site without replacing expensive hardware or components
- 200 event audit trail stored in the lock
- Standard AA-battery-operated, stand-alone locks require no wiring

Indications

A green/red/yellow LED indicates the following:

Function	LED
Low battery warning	3 yellow flashes
Guest privacy	1 yellow flash
Access granted	1 green flash
Lock-out card accepted	1 green flash
Undo lock-out card accepted	3 green flashes
Misread/wrong card	1 red flash
Scheduled Access mode – open	1 green flash each second
Lock communication OK	1 green flash
LockLink error	1 red flash
Command card accepted	1 green flash
Battery connected, application program installed	1 yellow flash when program is installed
Battery connected, application program not installed	1 yellow flash when battery is connected
Cylinder tamper alarm active	1 red flash each second

Remote Controller

In this case, the lock controller is mounted in a box with a remote controller board, which in turn controls an opening device. An external power supply powers the remote controller. The following additional functions are implemented:

- Alarm output which is activated when the door is forced open (no power to strike) or tampering.
- Strike powered via relay
- Egress switch

Alarm triggering and Anti Tail Gating via door switch (reed switch). The additional functions are implemented on an additional printed circuit board.

The remote controller can be recessed or mounted as a box to a wall or other surface.

The remote controller shown is the VingCard classic.



Multi Output Controller™ (MOC)™

The Multi Output Controller is designed for controlling access to up to 7 external devices. A typical installations are inside lifts (connected to the lift electronics) and outside lifts (connected to the call button electronics.) The function of a MOC is to activate up to 7 relay outputs when a keycard is inserted. The relay outputs may be connected to external devices. The activation is based on the information on the access bit map on the keycard.

Programming of the unit is done via the LockLink.

The remote controller shown is the VingCard classic.



Mag-stripe Encoders

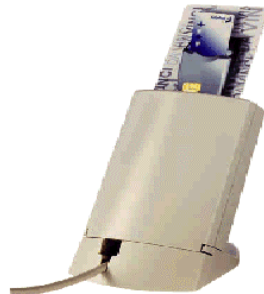
Mag-stripe encoders can be Single Track or Multi Track and can receive encoding information either via RS232 serial communications or direct from the Vision network using TCP/IP protocol. Serial encoders can also be networked by use of an intermediate serial server (such as the M200i) which converts from TCP/IP to RS232. The information used in the locks is encrypted and placed on track 3. Multi track encoders can also read and write information in standard ASCII format to tracks 1 and/or 2. A typical application is when a point-of-sale (POS) system needs to identify the keycard for a direct billing to an account.



Smartcard Encoders

Smartcard encoders are networked by use of an intermediate serial server (such as the M200i) which converts from TCP/IP to RS232.

As well as the extra security inherent with Smartcard technology, the extra memory capacity allows extra information – from or to the locks, or provided by third party partners – to be stored alongside the key-operation data.



VISION Software

The VISION software comes on a CD. The software can be installed on any PC running Windows 98, 2000, NT or XP.

Hardware Requirements

Most common brand PCs that meet the requirements for Windows 98, 2000 and NT can be used.

One PC must be used as the server. The server differs from the workstation in that it stores the data. Otherwise, the server and the workstations are the same regarding the VingCard VISION program.



Remember that you must have a sufficient number of COM ports to support serial encoders directly connected to PCs, the LockLink, and any RS232 PMS interface.

The requirements for the PCs are:

Windows 98/NT/2000/XP

- IBM PC or 100% compatible
- Windows 98/2000/NT SP4 or later/XP
- 64 MB RAM
- 2 GB HD space
- CD-ROM drive
- 2 COM ports

Lock Link

The LockLink consists of two primary components:

- A small palm top Windows CE/Pocket PC compatible computer

- The Contact Card for insertion into the locks, with cable and connection to the Pocket PC – and if necessary the Power-up unity (for emergency door opening)

The LockLink brings information from Vision database to the locks when the system is started for the first time (configuration and initialization) and brings information from the lock to Vision when a Lock Read-out is examined. The read-out information is also available directly from the LockLink where it can be viewed on the display screen.

The LockLink can also be used to unlock a door. If the lock's battery is discharged, the Power-up unit must be connected. In order for LockLink to unlock doors, the LockLink must be authorized from Vision in advance. The selected rooms can then be opened during the following hour.



Basic System Operations

One of the main advantages of the Vision system is the ability to encode of keycards to assign new access as well as to automatically remove access from older keycards. When a new guest keycard is inserted in the lock, the former guest's keycard is automatically "overridden" and can no longer open the lock. The keycard is only valid for a specified number of days (determined when the keycard is encoded) so that even if another guest is

not assigned to the same room or suite, the keycard would no longer be able to open the lock after the expiration date.

Employee keycards work in parallel with the guest keycards. The employee keycards also are valid only for a specified amount of time. However, it is usually for a longer time than a guest keycard. Employee keycards are normally issued for access to one or several sections of rooms, depending on the hotel's needs, but keycards for bellboys can easily be encoded to allow access to individual rooms, like guest keycards. Employee access keycards do not override guest keycards and therefore do not affect a guest's access.

Override Criteria

The process of having a keycard automatically override (invalidate) an existing keycard is a unique and patented feature of the Vision system.

The Override Criteria is normally determined by "Issue Time" (when the keycard was encoded.) An exception to this would be for situations such as cruise ships that issue keycards in advance. In this situation, they would probably want to use the "Start Time" (when the keycard becomes valid) rather than the Issue Time to be used as the Override Criteria.

To allow maximum product flexibility, a keycard can also be set up NOT to override another keycard. Keycards can even be set up to override *themselves*, resulting in a keycard that can only be used once (for example for a repairman to be able to enter a guest room once.)

Keycard Issue Time as override criterion:

This is the normal override criterion in a hotel situation. Most often, keycards are not issued until the guest has arrived, and an encoded keycard is valid immediately. A new keycard will override an existing valid keycard when it is used in a lock.

NOTE: Each hotel determines which keycards will override which other keycards. For example, a guest keycard will normally override another guest keycard, but a maid keycard will not override a guest keycard.

Keycard Start time as override criterion

This is the normal override criterion in ships, ferries, cruise liners etc. The reason for this is that keycards are often encoded prior to guest arrivals. A keycard will only override another keycard if its start time is later than the former keycard.

Flexibility/Configurability

A Vision system keyword is flexibility. The system and the locks can be configured to suit varying demands in lock plans, interaction between keycard Types, User Groups and Sections/Common Doors. Individual names of User Groups, Keycard Types, Sections, Time Tables, etc. can be selected in the System Setup Module. Locks are organized by groups with identical lock parameters. Lock parameters can be adjusted with respect to lock mechanisms and opening times etc. This makes it possible to control a large variety of lock devices.

Please also note that Vision supports the Escape/return lock function. If your facility has installed the Escape/return option, the facility must be fitted with STRATOS style lock cases.

Lock Modes

Locks can be set to operate in 3 different modes.

Normal Mode—the door is locked and unlocks when a valid keycard is withdrawn.

Passage Mode—the door will alternate between locked and unlocked whenever a valid keycard is inserted

Lock Open Time Mode—the door is set to automatically unlock and lock according to a preset Time Table. When the lock is in locked position, a valid keycard will open the door. In unlocked position, a green light is operative to show that the door is unlocked.

Keycard Types

The access structure is based on the concept of Keycard Types, such as "First Floor Maid" or "Guest". You can have up to 30 of these Keycard Types with each sharing the same Override Criteria and general access capabilities.

Virtually any access structure can be set up in the Vision system. Keycard levels can be created, but there is no need for a hierarchical keycard level structure. Almost any realistic lock plan or structure can be set up.

Sections

Sections are groups of doors. Access to doors in Sections is determined by checking whether the keycard has not expired or has been overridden by another keycard.

Common Doors

Common Doors are typically perimeter doors, garage, health club, pool, VIP floors etc. This access is assigned automatically when the keycards are issued based on the settings in the System Setup Module. Up to 53 of these Common Doors can be specified in the Vision system.

Access to Common Doors is given in addition to doors that are specifically selected when the keycard is issued and up to 16 Common Doors can automatically assigned to a keycard when it is issued. For example, all Guest keycards might automatically include access through exterior entrances and parking.

NOTE: Access to doors that have been designated as Common Doors is NOT overridden by other keycards.

Void-list™

A void-list in RAM, with a capacity of 20 user ID codes, can be used to immediately cancel individual keycards in a lock. The void-list keycard is used for this purpose. The voidlist-keycard can contain up to 5 user IDs to be void-listed.

Time-control

Time window

All keycards include a start and expiration date. The highest resolution is 30 minutes, allowing a 1-month time window. The lowest resolution is 12 hours, allowing a 2-year time window. Keycards can be issued one year in advance (depending on your PMS software) with any resolution.

Time Tables

In the system there are seven Time Tables defined by the hotel, plus one called "All Week" that has been created for you. The time is specified in 30 minute intervals. Access to each Access Area is restricted to the specific Time Table for the keycard.

In addition, a lock can allocate one of the Time Tables to toggle itself between open and keycard operated according to the Time Table. This is called the Lock Open Time Mode.

Interrelation™

Interrelation is another patented VingCard feature. Any Keycard Type may be interrelated or used as completely independent Keycard Types. Interrelated keycard mutually lock each other out. Guest, Suite and Fail-safe keycards are normally interrelated. The use of a new guest keycard will automatically lock out the previous guest's keycard.



If Guest, Suite, and Fail-safe Keycard Types are interrelated, use of a new Guest keycard will not only lock-out all previously used Guest keycards (normal operation for all Keycard Types) but all previously used valid Suite and Fail-safe keycards as well.

The interrelations of Keycard Types allow a room to be used as part of a suite of rooms for one guest, yet as a single room for another guest without requiring manual reconfiguration of the lock. Interrelated fail-safe keycards provide a system backup that does not require re-programming of the lock for each use.

Unique User Identification

Every issued keycard contains a **Unique User ID** code. This user ID code can be used to identify hotel employees in their use of the locks. The code will also make it possible to distinguish between different current hotel guests – even those sharing a room. This means that keycards can be individually changed or replaced with no knock on effect on other keycard holders. The Vision database contains names and cross-references to the user IDs. For employees, the name is used as identification both in keycard issuing and event reporting.

User Groups

Up to 256 User Groups can be established in the system. Each User Group consists of a combination of Sections and Common Doors with corresponding Time Tables. For each Keycard Type, the User Group determines a Time Table as an additional time restriction. User Groups simplify keycard issuing by limiting the number of individual selections which otherwise would have to be made every time a keycard is issued.

User Groups may typically be VIP guest, Regular guest, Maid 2. floor - day shift, etc.

Each user group has keycard family (mag-stripe or smart card) assigned to it, which determines which type of keycard will be made for members of that user group.

Cylinder for Mechanical Override (Optional)

Each lockset (apart from Presidio) may be equipped with a mechanical cylinder operated by the metal Emergency key (EMK). This cylinder will withdraw both latch and deadbolt when operated, and represents a dual independent emergency opening system, totally separated from the electronic lock controller.

The metal cylinder is recodable. The cylinder can be re-encoded twice in the event that the key is lost. Recoding of the cylinder requires use of the special Recode key which is included in the system package.

System Events

The Vision system keeps a constant log of every computer transaction. The log is recorded to the hard disk. The log may be recalled from computer memory at any time by running a system event report. Reports may include every computer entry or may be limited to a given room or a given user. Logged data are time of event, name of operator and details about the command issued.

Lock Readout

Up to 100 door entries are stored in the VC3000 Classic lock, up to 200 in DaVinci / Presidio lock - all can be displayed and examined by the LockLink, and transferred to the Vision system for a full print-out. For Locks capable of reading Smart Cards, lock events can also be transferred to Vision by a special **Readout** card.

The information about each entry is

- User ID code + Issue Area code
- Time of the event
- Value of override criterion (issue time, start time or end time)

The readout is a valuable tool both in prevention of crime as well as investigation of crime.

<p>NOTE: The Lock Event readouts are often used to prevent false accusations of hotel personnel.</p>

Other Functions

Lock-out

Lock-out keycards are issued to specific employees (usually maids) and they are normally used to prevent guests from returning to a room between the time they check out and the time their keycard expires.

When the room is cleaned, the maid can use the Lock-out keycard on the door. Then, only new guests will be able to open the door. This will ensure that the room will remain clean until the new guest checks in.

Whenever a Lock-out keycard is made, an Undo Lock-out keycard is also made. The Undo Lock-out keycard reverses the action of the Lock-out keycard and is normally only used if the guest has not actually checked out.

Deadbolt override

A keycard can be authorized to override the deadbolt. Certain User Groups can be pre-defined to always have Deadbolt override. For Guest Keys it is also possible to set Deadbolt override as a tick off item in the Common Door list box.

Fail-safe keycards

Sequential and Fail-safe Programming keycards are pre-made keycards, created so that if the computer ever goes down, you can use them as guest keycards. You should always keep the Fail-safe keycards available, in the event that the power goes out or for any reason the computer is not working.

NOTE: Before a Fail-safe keycard can be used as a valid guest keycard, another special keycard called a Fail-safe Programming Key must first be used on the lock. See the Help topic “About Programming Fail-safe Keycards” for more information.

The Two Methods of Implementing Fail-safe keycards

There are two methods of implementing Fail-safe keycards:

Random—This method creates Fail-safe keycards that can be used for ANY door. However, when the guest checks in, you will need to use a Fail-safe Programming Key and then a Fail-safe keycard on the door before giving the Fail-safe keycard to a guest.

Sequential—This method lets you create up to 8 Fail-safe keycards for each SPECIFIC door. Using this method, you go to each door with the Fail-safe Programming Key and then a Fail-safe keycard when you make them, so that they are ready to give to a guest if the computer system ever goes down.

Advantages and Disadvantages of each Method

Random method Fast to create –No need to use Fail-safe Programming Key until guests arrive. As guests arrive, you will need to use the Fail-safe Programming Key in the lock before using the guest’s Fail-safe keycard. If there is a power outage, you may not have enough employees available to do this. Also, if you did not make enough Fail-safe keycards, you may run out.

Sequential method Check in is easier –Just hand the guest their room key. Also, you will have enough Fail-safe keycards as they made for each specific room. Takes a little longer for initial setup as you will need to go to each door with the Fail-safe Programming Key to activate the guest’s Fail-safe keycard. Also, you will need to keep track of which doors the keycards are made for.

Fail-safe Programming keycards

Fail-safe Programming keycards instruct a lock to allow Fail-safe keycards to be used as guest keycards.

They are always used as the first part of a two-step process, with either Random or Sequential Fail-safe keycards. First, the Fail-safe Programming Key is inserted to tell the lock to allow a Fail-safe keycard to work. Then the Random or Sequential Fail-safe keycard is inserted. At this point, the Fail-safe keycard becomes a valid guest keycard.

If you are using Random Fail-safe keycards, you will not use the Fail-safe Programming Key until you check in guests. If you are using Sequential Fail-safe keycards, you will use the Fail-safe Programming Key on each room when the Sequential Fail-safe keycards are made, so that the guest can be checked in without any last minute effort.

You should always keep the Fail-safe Programming Key available in the event that the computer is down.



Anyone with a valid Fail-safe keycard and the Fail-safe Programming Key potentially could gain access to any door, so be certain to store the Fail-safe Programming Key in a secure place.

Programming Fail-safe keycards expire 2 years from the date they were created. Always make a new Fail-safe Programming Key before the old one expires.

System Configuration Examples

The Vision system can be configured based on your needs. The following examples show the various ways the system may be set up.

Single User System

You might want to use this configuration for situations such as a hotel with only one computer that will be used to issue keycards and manage the system settings. You could also select this if you want to install the Demo database on a computer for purposes of learning how the system works.



The example worksheets in Chapter 3 are based on the data in the Demo database.

Multi User System

This configuration is used if you have several workstations that will be used to issue keycards. They will be networked together and the server will contain the system databases.

PMS Interfaced System

The Vision system and the PMS system run on **different** hardware and Vision receives commands from the PMS system, either via a cable between the com ports of the two systems or using TCPIP protocol over a common network. The PMS interface is turned on/off from the System Setup module.

PMS Integrated System

The PMS system runs on the Vision server PC and sends commands programmatically.

PMS Display Modes

In a PMS Interfaced or PMS integrated system functions, one of 4 "Integration Modes" can be selected.

The 4 display modes affect what the user will see when they are encoding a keycard:

Silent - The PMS software interface is used. Only the VingCard logo is displayed when running. The only indication to insert a keycard for encoding, is the green light on the encoder.

Windows - Windows settings are used to determine how the message to insert a keycard is displayed.

Touch Screen - The Guest Keycard Module will appear. Unless they want to change any of the encode settings, all that is necessary is to touch (or click is using a standard monitor) the Encode button.

Full Vision - This is the recommended setting. It integrates with the PMS but also allows the person making keycards to access all of the Vision keycard encoding options.

NOTE: The Full Vision mode is recommended so that all of the Vision functions can be accessed.

The Vision Licensing Agreement

The software on the Vision installation CD is licensed to a specific end user. The license is your proof of license to exercise the rights granted herein and must be retained by you.

For more information about VingCard's licensing policies, please contact customer service at +47-66 81 40 00 or email us at service@vingcard.com.

NOTE: The Software is owned by VingCard and is protected against copyright laws and international treaty provisions. Therefore, you must treat the software as any other copyrighted material, except that you may either make one copy of the software solely for backup and archive purposes.

Single Licenses

The *Single License* VISION Software License Agreement permits use of one copy of the VISION software product on more than one computer, provided the software is in use on only ONE computer at any time.

Multiple Licenses

The *Multiple License* VISION Software License Agreement is always for a specific maximum number of users. It permits use of as many copies at one time as you have licensed.

Vision Basic And Vision Advanced

Vision comes in two variants : **Vision Basic** and **Vision Advanced**.

Vision Basic provides full functionality but limits the amount of Doors, User Groups, Timetables and Access Points that can be defined. It is suitable for smaller installations. PMS interface is supported for RS232 only.

Vision Advanced is a full version suitable for any installation. All PMS interfaces (RS232, TCPIP, DLL integration) are supported.

Feature	Vision Basic	Vision Advanced
Maximum number of Locks	300	10000
Maximum number of User Groups	32	256
Maximum number of Time Tables	4	8
Maximum number of Access Points (Common Doors)	4	53*
PMS RS232 support	Yes	Yes
PMS TCPIP support	No	Yes
PMS DLL Integration support	No	Yes
Batch mode Card Printing	No	Yes

* If you add use the More Rooms feature to give a mag-stripe keycard access to additional rooms, the number of available Access points will be reduced as follows :

1 extra room : max. 48 access points + 1 bit for VingCard Safe option

2 extra rooms : max. 13 access points + 1 bit for VingCard Safe option

See Chapter 5 (Setup > Locks Wizard > Common doors) for more details.

You can see whether you have **Vision Advanced** or **Vision Basic** installed by going to **System Setup > License**.

If you need to upgrade from **Vision Basic** to **Vision Advanced**, you can contact VingCard or your Vision representative to purchase an upgrade. You will be issued with a new set of License codes.



If you attempt to exceed any of the above limits (for example by adding too many locks in the System Setup Module), an error message will be displayed.

How to Upgrade capability with a new License code

NOTE: You will need to receive a new encrypted number from VingCard *prior* making the following changes to your system.

Follow these steps to upgrade

Select the **License** button from the main screen of the **System Setup** module.

Type in your new number from VingCard into the blank field.

Click **OK**.

You will now be able to add additional locks from the System Setup module.

Key to License Screen

Caption	Meaning
EV/ES Number	This number is assigned by VingCard. It was entered when Vision was installed. It is used as the product license number.
Facility Code	Each hotel has its own unique Facility Code. It is used to identify the property. Keycards issued from one Facility Code are not valid in any other Facility Code.
New Code Entry	Enter your upgrade code here

Chapter 3 : Planning the System

Overview of System Planning

Setting up and customizing the system determines who can access which doors at what times, who can issue keycards, and who can use which Vision software modules.

This section and the six worksheets are designed to help you determine the information that you need to set up the system before you begin designing it. It is not absolutely essential for you to follow the procedures outlined here, but you will find setting up the system much easier if you have completed the worksheets presented in the next pages. Filling out the worksheet properly and in the correct order is therefore **highly** recommended. It is also important as documentation of the installation and setup.



This chapter contains examples of filled-in forms as well as blank forms that you can copy and use for your own setup information.

As an alternative, you can create your own forms using spreadsheet software (or any other software you prefer.)

If you are setting up the system for the first time, use the forms in the following order:

Time Table Worksheet

You can have up to eight system Time Tables. The “All Week” which has been created for you and seven others that you can define. Time Tables are assigned to User Groups and Custom Doors. (For a blank worksheet, see *Time Tables Worksheet* on page 55.)

Common Door Worksheet

This worksheet is used as a preparation to define the Common Doors. (For a blank worksheet, see *Common Door Worksheet* on page 56.)

Keycard Type Worksheet (for all doors that are not Common Doors)

The lock plan is used to decide Keycard Types and the corresponding Access Areas. This data is used to create the complete lock plan in the system by allocating Keycard Type to different users. (For a blank worksheet, see *Keycard Type Worksheet* on page 57.)

User Group Worksheet

This worksheet is used to determine User Group names and associate them with Keycard Types, Time Tables, and Common Doors. (For a blank worksheet, see *User Group Worksheet* on page 58.)

System Parameters Worksheet

This worksheet is used to plan system default values, as well as all lock parameters for the different door groups in the system. (For a blank worksheet, see *System Parameters Worksheet* on page 59.)

Software Access Groups Worksheet

This worksheet will help you to create Software Access Groups which determine who has access to which software modules. In addition, you will define which Access Groups can issue which Employee Keycards. (For a blank worksheet, see *Software Access Groups Worksheet* on page 60.)

Worksheet Examples

This section gives an example and explanation of each of the worksheet forms after being filled in with data. The examples that are used are based on the "Demo" database which can be selected for installation for training or demonstration purposes.



In a normal working environment, an empty database will be installed instead of the Demo database. This will allow you to use your own data when setting up the system.

Defining Time Tables

Before determining Time Tables you need to decide how you want to restrict the access of guests and employees for different areas on a **time** basis.

Later you will be able to select from these Time Tables to assign them to **Custom Lock Groups** and to **User Groups**. Therefore, when you create Time Tables, you need to consider access based on time for both User Groups (all keycards belong to a User Group) as well as for Custom Locks such as lifts and parking.

Custom Locks can be set to work in Internal Control Mode which will automatically cause them to become unlocked or locked at predetermined times of the day (see Chapter 2 for an explanation of Lock Modes). The Internal Control Modes use the selected Time Tables to change from unlocked to keycard operated.



Specify as many of the Time Tables as you can at this point. Later, when you assign Time Tables to Custom Lock Groups and to User Groups, you can add more or make changes to your Time Tables.

Time Table Worksheet Example

Example:

Time Table 1: **All Week** 00:00 - 24:00

Time Table 2: **8-16**
8:00-16:00 every day except Sunday
Sundays 9:00-15:00

Time Table 3: **15-24**
15:00-24:00 all days

Time Table 4: **9-18**
9:00-18:00 all days

Time Table 5: **7-21**
7:00-21:00 all days

Time Table 6: **6-24**
6:00-24:00 all days

Up to eight Time Tables exist in the Vision system. Time Table no. 1 is the default "All Week" Time Table. It was created for you and is always one of the available Time Tables.

The remaining seven are defined by each hotel when the system is set up. Each Time Table specifies the time for each day of the week.

Time can be specified in increments as small as 30 minutes. For example, 12:30 would be acceptable, but 12:15 would not.

Below you see an example of a completed Time Tables Worksheet. In this example, the hotel determined they only needed to define 5 new Time Tables to suit their needs (the All Week Time Table is built into the software).



- In the example, the Time Tables are named based on the times used. However, you can name them whatever you wish. For example "Night Shift" or "Common Door".
- A 24 hour clock was used in the Time Table example, but if you prefer, you can specify the time as a.m. and p.m. For a 24 hour clock, use 00:00 to 24:00. For a 12 hour clock, specify the time as a.m. and p.m.

(For a blank worksheet, see *Time Tables Worksheet* on page 55.)

Time Tables Worksheet Example

	Time Table Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat
1.	All	00:00-24:00	00:00-24:00	00:00-24:00	00:00-24:00	00:00-24:00	00:00-24:00	00:00-24:00
2.	8-16	09:00-15:00	08:00-16:00	08:00-16:00	08:00-16:00	08:00-16:00	08:00-16:00	08:00-16:00
3.	15-24	15:00-24:00	15:00-24:00	15:00-24:00	15:00-24:00	15:00-24:00	15:00-24:00	15:00-24:00
4.	9-18	9:00-18:00	9:00-18:00	9:00-18:00	9:00-18:00	9:00-18:00	9:00-18:00	9:00-18:00
5.	7-21	07:00-21:00	07:00-21:00	07:00-21:00	07:00-21:00	07:00-21:00	07:00-21:00	07:00-21:00
6.	6-24	06:00-24:00	06:00-24:00	06:00-24:00	06:00-24:00	06:00-24:00	06:00-24:00	06:00-24:00
7.								
8.								

Defining Common Doors

Locks can be specified as Common Doors. Typically they will be locks such as parking, swimming pool, exterior doors, and so on. The purpose of specifying locks as Common Doors is that Common Doors "behave" differently than doors such as guest room doors. In guest room doors, a new guest's keycard overrides the previous guest's keycard and makes it invalid in the lock. In Common Doors the previous keycard's access is **not** overridden by a newer keycard. Therefore you can assign an unlimited number of keycards access to the locks at the same time.

Another difference between Common Doors and other doors is that they will automatically be assigned to a keycard based on the **User Group**. This means that unlike assigning a room to a guest, which requires you to select a specific room number, the Common Doors are assigned automatically. This simplifies making keycards because when you check in a guest or make an employee keycard, the Common Doors will be assigned automatically (based on the User Group).

Later in this chapter you will determine the User Groups and assign Common Doors to them.



There is no limit to the number of different keycards that can be given access simultaneously to a Common Door.

Defining Common Doors

All Common Doors are defined as one of these two Common Door Types:

- Standard Lock/Remote Controller (**usually main entrance, parking, and so on**)

—OR—

- Lift Controller/MOC (**usually elevators or parking areas with 7 relay contacts**)

<p>NOTE: The maximum number of Lift Controller/MOCs per installation is 7.</p>



The terms "Lift" and "Elevator" are interchangeable.

When setting up the Lift Controller/MOC, it is possible to select which of the 7 Relay Contacts will be included with each Lift Controller.

The Common Door Worksheet contains two columns, one for the Common Door Name and one for the Common Door Type.

Common Door Example

In the following example, 3 Standard Lock/Remote Controllers and 2 Lift Controller/MOCs were specified. (For a blank worksheet, see *Common Doors Worksheet* on page 56.)

Common Doors Worksheet Example

Common Doors	Common Door Type
Parking	Standard Lock/Remote Controller
Fitness center	Standard Lock/Remote Controller
Backdoor	Standard Lock/Remote Controller
Lift 4 th floor	Lift Controller/MOC
Lift 5 th floor	Lift Controller/MOC

Keycard Type Worksheet (Defining Doors that are not Common Doors)

After you have defined all of your locks that are Common Doors (previous section), use the **Keycard Types** form to specify information for all of the remaining locks.

There are 5 elements you must specify for each of the locks:

- **Keycard Type**—general categories based on who will have access. You can name them yourself using the example as a reference.
- **Lock Group**— must be defined as one of the following:
 - guest room
 - guest suite
 - employee room
 - employee section
- **Access Area**—Access Area is a set of doors. Up to 10 Access Areas can be assigned per Keycard Type.
- **Override Criterion**— must be defined as one of the following:
 - Issue Time (IT)
 - Start Time (ST)
- **Interrelation to Itself and Other Locks**—specify whether this Keycard Type will invalidate itself and whether it will invalidate Keycard Types in other locks

Keycard Type

You can have up to 30 different Keycard Types. Typical employee Keycard Types are Maid, Housekeeper, Room Service etc., but guests may also be divided into Keycard Types such as Suite guest, Regular guest etc.

NOTE: When rooms in a hotel can be combined to make suites, one Keycard Type must be allocated to each suite configuration.

NOTE: If you have set up Keycard Types with identical names and overlapping sections, such as two housekeeper Keycard Types, one for Floor 1+2 and another for Floor 2+3, they are in reality of different Keycard Types for the system. Be careful that you interrelate the correct Keycard Types in this case.

Defining Locks Included in Keycard Type

The building blocks for **Locks Included in Keycard Type** are room numbers. They can be defined either as a range of locks or by several single locks.

Example:

Our example hotel has 4 Floors (1- 4). Each floor has 4 rooms. The first two rooms on Floor 1 and 2 can be also combined into a suite. In addition, there are linen closets on each floor called Linen1, Linen 2, Linen 3 and Linen 4. The hotel will be set up to have the following Access Areas:

Suite1= 101,102 (suite defined as room 101 + room 102)
 Suite2 = 201,202 (suite defined as room 201 + room 203)
 maxisuite1= 101,102,103 (suite defined as rooms 101-103)
 maxisuite2= 201,202,203 (suite defined as rooms 201-203)
 Floor1 = 101-104(all defined rooms on 1. Floor)
 Floor2 = 201-204
 Floor3 = 301-304
 Floor4 = 401-404
 Linen1 = Linen1 (defining a single door as an Access Area)
 Linens = Linen1- Linen4
 all rooms = 101-104, 201-204, 301-304, 401-404
 entire hotel = 101-104, 201-204, 301-304, 401-404,Linens

Specifying Suites

The flexibility of the Vision system gives you a powerful tool to handle various suite combinations. Suites are of Lock Group **Guest Suite**. Non-overlapping suites (such as 101+102, 103+104) have to be set up as one Keycard Type element each, as shown in the filled-in worksheet. If suites are overlapping (such as 101+102, 102+103) two Keycard Types will be allocated in Lock 102.

All suite combinations must be set up in the system separately.

Allocation Of Keycard Type
 In the above example, 13 Keycard Type will be allocated. They are:

- 1 for Guest single room
- 1 for Guest Suite
- 1 for Guest Maxisuite
- 1 for Vendor
- 1 for Bellboy
- 1 for Maid
- 2 for Housekeeper
- 2 for Room Service
- 1 for Engineering
- 1 for Management1
- 1 for Management2

Override Criterion

The purpose of keycards overriding other keycards is to prevent access by an older keycard. (hotel industry) or to prevent access by a keycard with a later start date (cruise industry). For example, when a new guest uses his keycard to open his room door, the previous guest's keycard immediately becomes invalid in the lock. Because of this, it is normally not

necessary to do anything to remove access from guests who have checked out, even if their keycard has not expired.

The Override Criterion is based on either the point of time when the keycard was issued or the start time (ST) of the keycard (when it becomes valid). Issue Time (IT) is the normal Override Criterion in a hotel situation. Start Time is the normal Override Criterion in ships, ferries, cruise liners etc.

Defining Interrelations

Keycards may be set up to invalidate other keycards in some locks. This is called Interrelation. Interrelation is a powerful tool to control how keycards for different Keycard Types interact. The Interrelations are defined when the system is set up.

In the preceding example, the suite and guest-Keycard Types need to be interrelated so that when a new guest is checked into a room, the previous guest will no longer have access.

NOTE: The fail-safe Keycard Type, which is in the system by default, also has to be interrelated to all guest Keycard Types.

A Keycard Type can also be interrelated to itself, thus automatically making itself invalid in a lock after the first use. In the example, the bellboy Keycard Type should be marked to interrelate to itself.

Interrelations may be represented in a Keycard Type/Keycard Type table as shown below. Read the table by rows. New keycard of Keycard Type Guest single room will cancel Guest Suite, Guest maxi-suite, Fail-Safe (but not Guest Floor suite). New keycard of Keycard Type Guest Floor Suite will cancel Guest single room, Guest Suite, Guest Maxi Suite and Fail-safe.

Defining Lock Groups

Examples:

Bellboys with access to individual (determined when keycard is issued) rooms: Lock Group = **Employee Rooms**.

Guests with access to individual rooms (variable on issuing): Lock Group = **Guest Rooms**.

Guests with access to combinations of rooms, such as suites: Lock Group = **Guest Suites**. (Each suite combination has been predefined in the Keycard Type Worksheet.)

Maids with access to sections, such as maid 2. Floor: Lock Group = **Employee Sections**. When a keycard is issued, the User Group limits the availability of sections to 1.

If a Keycard Type has been defined as Lock Group "Rooms", the system will make all rooms in the area available as individual rooms for the defined Keycard Type.

The system differs between Employee and Guest Keycard Types. If a Keycard Type has been defined as Lock Group "section" (Employee) or "suite" (Guest), the system will make a section/suite of rooms available as individual selections for the defined Keycard Type.

All Lock Groups (except Lock Group Employee Section) have **variable** Access Areas. If the Access Areas are variable for a Keycard Type, you can select the Access Area when the keycard is issued. If the Access Area is fixed, as for Keycard Types with Lock Group Employee Section, the keycard will automatically be issued for the pre-selected Access Area(s).

NOTE: allocating specific lock types to locks within a lock group

All locks within a lock group DO NOT have to be of the same type – that is, locks are generally grouped by function (“Guest rooms” rather than by hardware type “Da Vinci”). For example, lock group GuestRooms might contain both VC3000 classic locks and Da Vinci locks. Perhaps the Da Vinci locks are all located on floor 4 and are intended for use by VIP Guests issued with Smartcards. Within Vision setup for the GuestRoom lock group, floor 4 locks are then set up as type ‘Da Vinci combo’ and all other Guest Room locks as type ‘VC300 Classic’ (=mag-stripe only).

In this way, the number of Lock Groups and Keycard Types need not increase simply due to a mixing of card technologies, yet Vision is still able to ensure that only valid keycard types are made for each room. For example, you would only be able to make a Smartcard for a guest staying on floor 4 (DA Vinci combo locks).

Keycard Type Worksheet Example

In the Keycard Type Worksheet, every Keycard Type is assigned an Access Area.

Normally you want the same Keycard Type to have access rights to several sections: one group of the employees belonging to a Keycard Type "Maid" might have access to Floor1 only, another to Floor2 only. In this situation, you fill in a line for each of these “groups”, reflecting how this is done at the actual setup. Each line will represent a **Keycard Type Element**.

NOTE: The maximum number of Keycard Types is 30, while the limitation for Keycard Type elements is significantly higher and limited only by the available system memory.

You can allocate a maximum number of 10 Access Areas to each Keycard Type Element.

The Keycard Type “Guest” covers all guest **User Groups**.



In the following example, **IT**=Issue Time and **ST**=Start Time.

In the form below, Keycard Type **Maid** has four Keycard Type Elements, Housekeeper has three, Room Service has three, and Engineering has one Keycard Type Element. (For a blank worksheet, see *Keycard Type Worksheet* on page 57.)

Keycard Type Worksheet Example

Keycard Type	Locks Included in Keycard Type	Lock Group	Over-ride	Interrelation	
				To Itself	To Others
Single rooms	100-120, 200-220, 300-320, 400-420	Rooms	IT		
Connecting 0/1	100+101, 200+201, 300+301, 400+401	Suites/Connecting	IT		
Connecting 0/2	100+101+102, 200+201+202, 300+301+302, 400+401+402	Suites/Connecting	IT		
Connecting 1/2	101+102, 201+202, 301+302, 401+402	Suites/Connecting	IT		
Suites	110-112, 210-212, 310-312, 410-412	Suites/Connecting	IT		
Employee Rooms	600-605	Rooms	IT		
One Shot Key	100-120, 200-220, 300-320, 400-420	Rooms	IT		
Housekeeper	All Guest Rooms, All Storage Rooms, Employee Rooms	Section	IT		
Maid	1 st floor	Section	IT		
Maid	2 nd floor	Section	IT		
Maid	3 rd floor	Section	IT		
Maid	4 th floor	Section	IT		
Maid 2 floors	1 st and 2 nd floor	Section	IT		
Maid 2 floors	3 rd and 4 th floor	Section	IT		
Maintenance	All Guest Rooms	Section	IT		
Master	All Guest Rooms, All Storage Rooms, Employee Rooms	Section	IT		
Minibar	1 st and 2 nd floor, 3 rd and 4 th floor	Section	IT		
Room Service	All Guest Rooms	Section	IT		
Security	All Guest Rooms, All Storage Rooms, Employee Rooms	Section	IT		
Banquet	All Meeting Rooms	Section	IT		

NOTE: The system will allow up to 30 Keycard Types.

NOTE: When a keycard is issued for a suite, use any of the room numbers included in the suite and make sure the keycard is issued to the correct Keycard Type.

Specifying Suites

The flexibility of the Vision system gives you a powerful tool to handle various suite combinations. Suites are of Lock Group **Guest Suite**. Non-overlapping suites (such as 101+102, 103+104) have to be set up as one Keycard Type element each, as shown in the filled-in worksheet. If suites are overlapping (such as 101+102, 102+103) two Keycard Types will be allocated in Lock 102. All suite combinations must be set up in the system separately.

Allocation Of Keycard Type
In the above example, 13 Keycard Type will be allocated. They are:

- 1 for Guest single room
- 1 for Guest Suite
- 1 for Guest Maxisuite
- 1 for Vendor
- 1 for Bellboy
- 1 for Maid
- 2 for Housekeeper
- 2 for Room Service
- 1 for Engineering
- 1 for Management1
- 1 for Management2

NOTE: Keycard Types may have same name and overlapping Access Areas. In that case, different Keycard Types will be allocated. *Make sure that overlapping is shown in the Access Areas (such as Floor1/Floor2 and Floor2/floor3). If they are hidden, they can only be revealed by the lock ID/Access Area link. This can be viewed in the system from System Access Areas.* In the above form, both Housekeeping and Room Service have overlapping Access Areas.

Defining User Groups

Up to 256 User Groups can be established in the system. Each User Group consists of a combination of:

- Keycard Type for the User Group
- The Card Family (for example, mag-stripe or smartcard) that will be issued for the User Group
- Access Areas with corresponding Time Table
- Common Doors with corresponding Time Table

User Groups are created for identical where-and-when-elements. User Groups represent a further structuring of the term Keycard Type as it distinguishes between users of same Keycard Type, but with different Time Tables and/or Access Areas – or with different types of Keycard. For example, VIP guests might have access to more common doors than regular guests and also be issued with Smartcards rather than mag-stripe cards.

NOTE: Unless you need to assign guests different Time Tables or Common Doors, or wish to issue Smartcards only to a limited sub-set of guests, you can create one User Group for all guests.

Filling in the User Group Worksheet

This worksheet illustrates the relationship between:

- Keycard Types
- Deadbolt Override
- Access Areas
- Time Tables
- Common Doors

For each User Group, select a Time Table for the Access Area as well as Time Tables for all selected Common Doors.

User Group Name

Each User Group needs a unique name.



User Groups are based on Keycard Types, so when determining User Group names, it is easiest if you use the corresponding Keycard Type and extend it with your own naming convention (based on the access and the Time Tables). For example, mdfl2night, hkffloor1+2 etc.

Keycard Type and Access Area

Fill in the assigned Keycard Types and the assigned Access Areas so that you will get a better overview.

NOTE: When setting up User Groups, you may decide that you need additional Keycard Types or Time Tables. If you do, return to the Time Table or Keycard Type worksheet and update it with the new names.

Time Table

Select one of the Time Tables for each **User Group**. For example, you might want to limit the use of night employees to evening hours.

You will also select a Time Table for each of the **Common Doors** that you want this User Group to be able to access. (see *Time Tables Worksheet Example* on page 40).

Duration

The duration for Keycard Types **Employee Section** will determine how long a keycard will be valid from the day it is issued. Note that the Start Time of a keycard in a certain section-type User Group is identical for ALL keycard holders. A new keycard holder will receive a

keycard with a previous Issue and Start Time, but with a different ID. Duration is by default two years for Employee Section Keycard Types.

Deadbolt Override

Use this column to denote whether or not the User Group should have a default Deadbolt Override.



Deadbolt Override allows a door to be opened even when the deadbolt is thrown, so you will normally not want most User Groups to have this type of access.



It is not necessary to specify Deadbolt Override capabilities for guest keycards or employee room keycards. The setting for whether Deadbolt Override will be an option when issuing keycards is specified in the System Parameters settings. It is set for *all* guest and *all* employee room keycards.

Card Family

Decide which type of keycard (mag-stripe or smartcard) you will issue for this user group. Be sure that all the locks you intend members of this user group to have access to can accept the type of card selected.

For example, if you want to issue VIP Guests with Smartcards and your VIP Guests will all use rooms on floor 4, then these rooms must be equipped with Smartcard compatible locks. If they are combo locks (that accept both mag-stripes and Smartcards) then the necessary staff can still gain access via mag-stripe cards.

Common Doors and Corresponding Time Tables

They should be listed in the User Group Worksheet under Common Doors with their corresponding Time Tables.

NOTE: The maximum number of Access Groups, which can be made available for one User Group, is 16 out of the whole range of 53.

In the Common Door columns, use the corresponding Time Table number. The User Groups assigned to Lock Group **guest room**, **guest section** or **employee room** will have the option of having up to 16 Common Doors listed as default when a keycard is issued, or just available on request. Mark the default possibility with a “d” next to the Time Table.



The User Groups assigned to Lock Group **employee section** will automatically have all Common Doors on by default.

The Start time (ST) and End Time (ET) for User Groups with Lock Group **Employee Section** are decided when the system is being set up, while ST and ET for other Lock Groups are decided when the keycard is issued. The system by default sets Start Time to the time the group is established in the System Setup Module.

Below is shown an example of a filled in User Group form. (For a blank worksheet, see *User Group Worksheet* on page 58.)

User Group Worksheet Example

User Group	Keycard Type	Dead-bolt	Time Table	Card Family	Common doors with time tables				
					Parking	Fitness Center	Backdoor	Lift 4th floor	Lift 5th floor
Banquet	Banquet	Off	1	mag			1		
Emergency	Master	On	1	mag	1	1	1	1	1
Employee Rooms	Employee Rooms	On	1	mag					
Housekeeper	Housekeeper	Off	1	mag		5	6	1	1
Maid day 1 st Fl	Maid	Off	2	mag			2		
Maid day 2 nd Fl	Maid	Off	2	mag			2		
Maid day 3 rd Fl	Maid	Off	2	mag			2		
Maid day 4 th Fl	Maid	Off	2	mag			2		
Maid night ½	Maid 2 floors	Off	3	mag			3		
Maid night ¾	Maid 2 floors	Off	3	mag			3	3	3
Maintenance	Maintenance	Off	5	mag		5	5	5	5
Master	Master	On	1	mag	1	1	1	1	1
Regular Guest	Variable **	On	1	mag	1	1		1	1
Room Service	Room Service	Off	6	mag			6	6	6
Security	Security	On	1	mag	1	1	1	1	1
V.I.P Guest	Variable	On	1	smart	1	1	1	1	1

Defining System and Lock Parameters

Several system and lock-related parameters must be set up during the installation. The system parameters are global in the sense that they are common to the system. The lock parameters are common for all locks inside one Lock Group.

The System Parameter Worksheet helps you to define both the system parameters and the lock parameters so they are ready and predefined when you go through the Setup commands in the system.

Lock Parameters

Locks are organized according to Lock Groups. A Lock Group can be one individual lock or a group of locks. Within a Lock Group, all locks have identical setup parameters. The lock

parameters are a set of data used to define the operation of each lock. Normally all guest room doors have equal parameters and a typical group may therefore be **Guest rooms**. Other groups may be common area doors, conference rooms etc.

The lock parameters are:

- Lock Group
- Lock Type
- Lock Motor Type
- Open Pulse Width
- Unlock Time
- Lock Mode
- Log Invalid Keycards

In addition, for each Lock Group you must define a Lock ID, and Internal Control Mode operation.

Lock Group

Select whether the lock(s) you are creating are for Guest Door Locks, Lift Controllers (elevators), or Custom (special settings).

Lock Type

Lock Type can be either VingCard or Custom. Use Customize only for special doors equipped with other locking devices than the VingCard standard lock case.

Lock Motor Type

You will need to specify the Duration and Pulse Width required by the lock.

Most often, these are devices connected to a remote reader. However, you may also want to select this for VingCard motors that require a longer or shorter pulse.

Open Pulse Width

You only need to fill in this information if the lock type has been defined as Customize. If the Lock Motor Type has been defined as **pulse**, this defines both open and close pulse. The pulse widths may be set between 20ms and 2550 ms in 10 ms steps.

Unlock Time

The Unlock Time defines how long the lock remains unlocked after a valid keycard has been withdrawn. It is the interval between open pulse and close pulse. The Unlock Time can be set to any number between 1 and 255 seconds. 6 seconds is default.

Lock Mode

You can set the lock to open and close according to either Normal Mode or Passage Mode.

- **Passage Mode**—Passage Mode is used when a lock is to automatically to be either locked or unlocked based on the Time Table.
- **Normal Mode**—In Normal Mode, the lock controller sends an open pulse as soon as a valid keycard has been withdrawn followed by a close pulse after the defined Unlock Time.

Log Invalid Keycards

The lock events include the last 100 events for VC3000 Classic lock or 200 for DaVinci / Presidio lock. If Log Invalid Keycards is set to Yes, unsuccessful attempts to unlock the door will also be stored.

Internal Control Mode

When a lock controller is set to work in Internal Control Mode, it switches from Normal Mode to unlocked according to one of the eight system Time Tables. Internal Control Mode is typically used for doors to Common Doors. Decide which Time Table to work with and fill in the form.

NOTE: Common Doors working as Lift Controller/MOCs are already predefined to fixed values in the system. No definitions need to be planned for these.

Lock ID

You must identify the locks that operate with the parameters as defined. The ID can be a name, a room number, or a range of room numbers.

System Parameters Worksheet

Part of the System Parameters Worksheet is used to fill in the lock parameter information. (For a blank worksheet, see *System Parameters Worksheet* on page 59.)

System Parameters Worksheet Example

	Default	Lock group name			
		rooms	confer.	Backdoor	VIP lift
Corresponding Lock IDs		all g.r.	B1	Backdoor	VIP lift
Lock Group (Guestroom/Other)		guestr.	other	other	other
Lock type (VingCard/Customize)		VC	VC	Custom	VC
Lock motor type (Pulse/Duration)		\	\	dur	\
Open pulsewidth (msec)	30 ms	\	\	300	\
Unlock time (1-255 seconds)	6 s	4	6	4	6
Lock mode (Normal/Passage)	Normal	normal	passage	normal	normal
Allowed to log invalid keycards (yes/no)	No	yes	no	no	no
Internal Control Mode (yes/no)	No	no		yes	no
Internal Control Mode Time Table (0-7)				2	

Defining System Parameters

For a description of all System Parameters, please see "System Setup Screens" in the Using Vision Software Modules chapter.

Default Check-in Time/Check-out Time

These defaults automatically are displayed when a keycard is issued. The operator can either accept the default times or enter another point in time.



If you set check-in time to 00:00, the current time will be selected as check-in time when you issue a keycard.

Default Length of Stay

The default length of stay in days determines the default check-out date based on the check-in date. If check-in date is Aug.18 and the default length of stay is two days, the suggested check-out date will be Aug. 20.

Default User Group

Select one of the defined User Groups with Keycard Type **Room** or **Suite** to be the default User Group that is displayed when keycards are issued.

Default Section (Keycard Type)

Pick one of the defined **Room** or **Section** Lock Groups to be used as the default when issuing keycards.

Issue Area Code

The Issue Area Code is encoded on each keycard to show where the keycard was issued. This is important where several computer systems are processing keycards for one facility. The default pre-setting of issue area codes is "0". If you want to use a non-default Issue Area Code to distinguish the system, specify a different number.

Inhibit Override

The inhibit override is by default set to "off". If inhibit override is set to "on", it means that issued keycards will NEVER override a valid keycard in the lock. Normally inhibit override is set to "off" only if the issuing computer system is not in any sense linked to the property where the keycards will be used.

Daylight Saving Time/Daylight Saving Time Dates

The information set up in the system about daylight saving time start and end is configured into the lock when it is programmed. If this date changes the locks must be reprogrammed.



The system automatically adjusts to the daylight saving times based on your Windows settings.

Workstation and Encoder Time Outs

The Workstation Time Out defines the number of minutes of inactivity to wait before logging out the current user. The Encoder Time Out specifies how long to wait when something is wrong (no card inserted, encoder not turned on, etc.) before aborting the encode instruction.

Deadbolt Override menu option

This option is turned on/off in the System Setup module and is a system-wide setting. If it is turned on, Deadbolt Override will appear as one of the Common Doors options when making keycards. If turned off, the User Group will determine whether Deadbolt Override is assigned to a keycard.

<p>NOTE: This setting affects guest keycards and employee room keycards only.</p>
--

Subtract hours

The specific number of hours to subtract from the keycard's issue time. If it is set to 0 hours, the system is compatible with earlier versions. The default is 1 hour.

Example: If set to 2 hours, each keycard will have an issue time that is two hours earlier than the time that the keycard was encoded.

Defining Software Access Groups

Access to Modules

You can create Software Access Groups and determine which Software Access Groups can access which software modules. For example, you might want to create a SAG called "Front Office" that can access only the modules that create employee and guest keycards.

Ability to Encode Employee Keycards

In addition to specifying which modules a Software Access Group can access, you can also determine which User Groups the Software Access Group can encode keycards for.

When employees choose Add or Change in the Employee Keycards module, the only employee names that will be listed are those that match the User Groups for the operator's Software Access Group.

Software Access Groups Worksheet Example

Software Access Group Name	Modules									Startup Module	Can Make Employee Keycards for these User Groups													
	Employee Keycards	Employee Rooms	Guest Keycards	LockLink	Maintenance	Reports	Special Keycards	System Setup	System Users		Banquet dept	Emergency	Employee room	Maid day 1st fl	Maid day 2nd fl	Maid day 3rd fl	Maid day 4th fl	Maid night 1/2	Maid night 3/4	Housekeeper	Maintenance	Master	Room Service	Security
Front Office Supervisor	x	x	x	x		x	x		x	guest	x		x	x	x	x	x	x	x	x	x		x	x
Front Office	x	x	x							guest	x		x	x	x	x	x	x	x					
Maintenance	x	x		x		x			x	guest	x	x	x	x	x	x	x	x	x	x				
Management	x	x	x	x	x	x	x			guest	x	x	x	x	x	x	x	x	x	x		x		
Vision Supervisor	x	x	x	x	x	x	x	x	x	setup	x	x	x	x	x	x	x	x	x	x	x	x	x	x

Blank Worksheet Forms

A blank worksheet for each form is contained in the following section. You can remove the page and make a copy of it to use to fill in the information for your hotel.

For examples of filled in forms and an explanation of each form see the corresponding section in this chapter.

Time Tables Worksheet

	Time Table Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat
1.	All	00:00-24:00	00:00-24:00	00:00-24:00	00:00-24:00	00:00-24:00	00:00-24:00	00:00-24:00
2.								
3.								
4.								
5.								
6.								
7.								
8.								

Common Doors Worksheet

Common Doors	Common Door Type

Keycard Type Worksheet

Keycard Type	Locks Included in Keycard Type	Lock Group	Over- ride	Interrelation	
				To Itself	To Others

System Parameters Worksheet

[illegible]

Software Access Groups Worksheet

[illegible]

Chapter 4 : Using LockLink

LockLink overview

The following figure illustrates the components of the LockLink and how it is connected to the PC (Vision workstation or server), Contact Card and power supply.

LockLink components



1. Pocket PC with Windows software
2. Docking station
3. Serial connector to Vision PC
4. Power supply
5. Contact Card for programming doors

The parts 1 to 4 are delivered as a package.

The Vision LockLink software can be installed from a PC (using Microsoft ActiveSync) or by plugging a pre-programmed Compact Flash card into the Pocket PC.

NOTE: The screen shots in this chapter are just examples. Real PocketPC devices may display different graphic and texts.

Installing the VISION LockLink software

The Pocket PC package does not have the LockLink software installed.

The Vision LockLink software is delivered on a CD. A license code is also delivered with the software, and this must be typed in at the end of the installation. Optionally, the software can be delivered on a Compact Flash card.

Before the LockLink installation can start, a few steps must be done to prepare the installation. This installation guide covers all necessary steps to make the Vision LockLink software run.

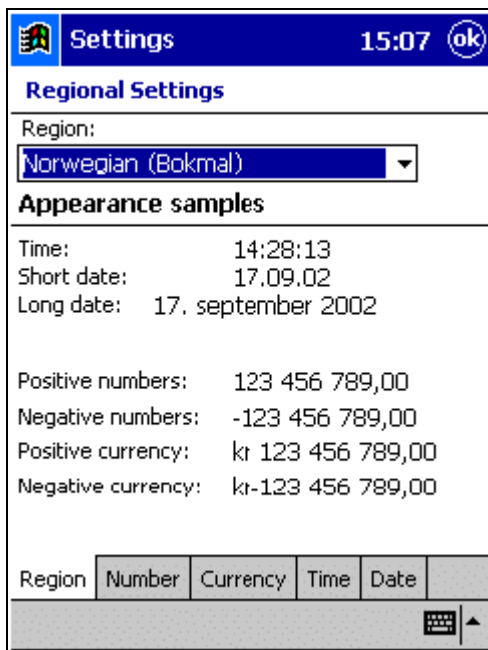
Quick Start Guide

Please refer to the “Quick Start Guide” that is delivered with the Pocket PC to set up the Pocket PC. This guide shows how to

- install batteries,
- power up the device,
- run the welcome wizard, and
- connect to the computer.

Defining regional settings

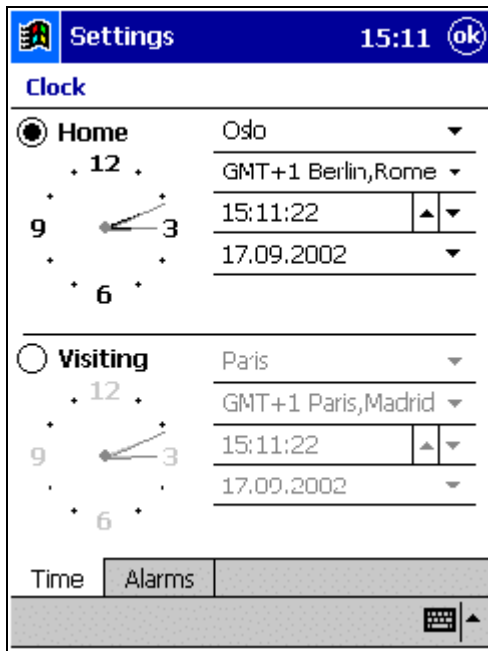
Before installing the LockLink, define the regional settings of the Pocket PC. To access the Regional Settings screen, select **Start/Settings/System/Regional Settings**. In the Regional Settings screen, select the appropriate region.



Setting clock

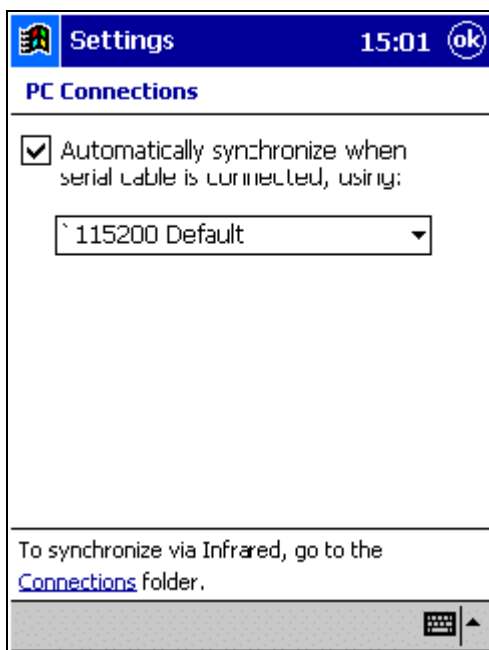
Next, set the clock of the Pocket PC to local time. To access the Clock screen, select **Start/Settings/System/Clock**. In the Clock screen, select your local time zone as “home” time. Note that Microsoft ActiveSync will also synchronize the LockLink clock automatically upon every connection to Vision.

NOTE: If the home region set on the Pocket PC does not correspond the regional settings on the VISION PC, the time in the LockLink will not be correctly set.



Defining PC connection

Set the baud rate of the serial connection to the DA VINCI workstation to 115 200 baud and check the ‘Automatically connect...’ checkbox. To access the PC Connections screen, select **Start/Settings/Connections/PC**.



Removing old LockLink version

If you have an old version of Vision LockLink installed on your system, it is recommended that you remove the old version before installing a new one. To access the Remove Programs screen, select **Start/Settings/Remove Programs**. To remove the old version of Vision LockLink, select **VingCard Vision LockLink** from the list and press **Remove**.

NOTE: Before removing the Vision LockLink, make sure that the application is not running.



Installing Microsoft ActiveSync

Microsoft ActiveSync must be installed on the workstation running Vision. This is a program that will handle communication between the PC running Vision and the Pocket PC, and synchronize the LockLink and the PC clocks. It is therefore important that you follow the installation instructions carefully. The program is delivered on a separate CD with the Pocket PC.

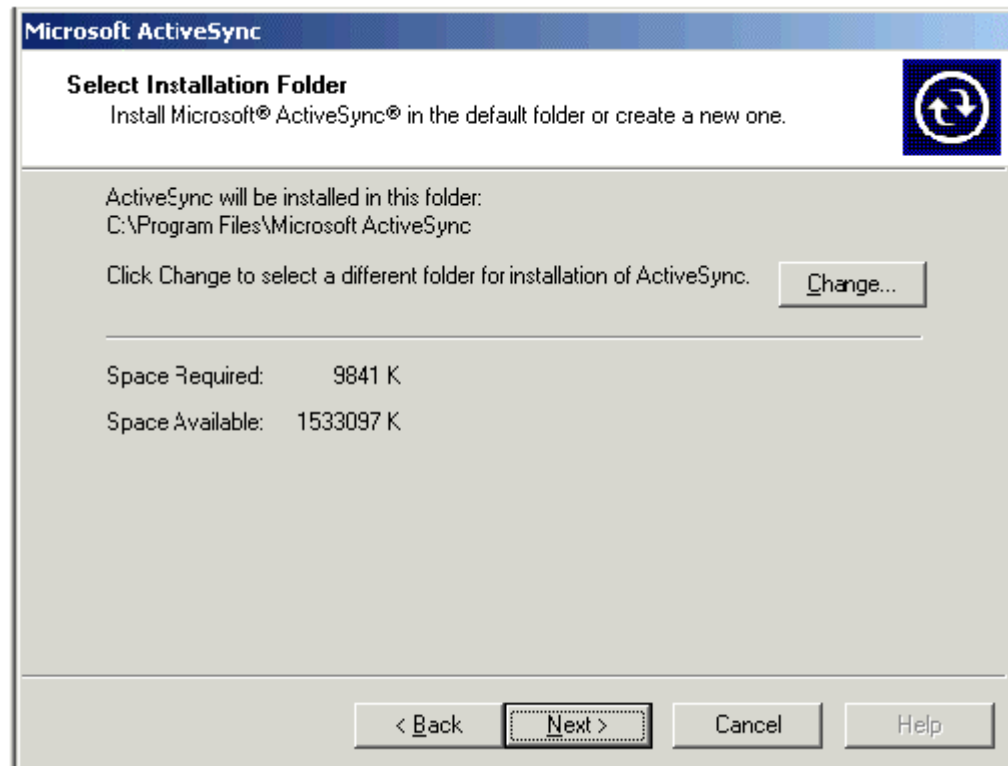
To install Microsoft ActiveSync, do the following:

1. Insert the ActiveSync installation CD into the CD-ROM drive of the workstation.

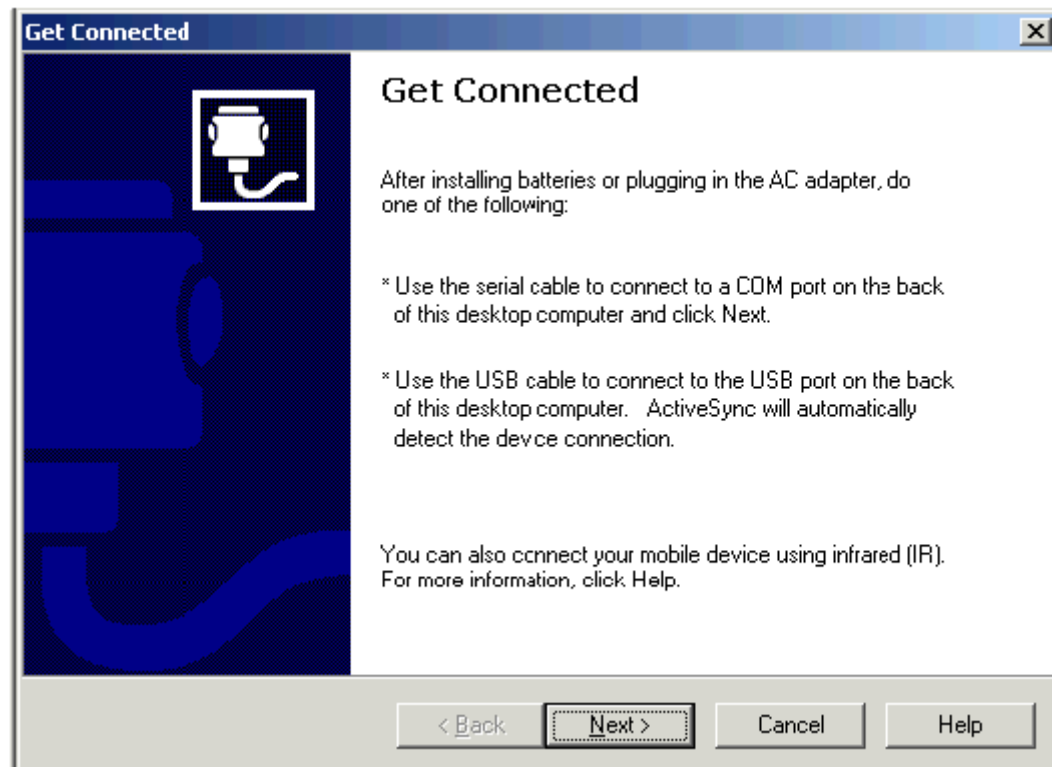
Microsoft ActiveSync is launched automatically. Press **Next** to continue.



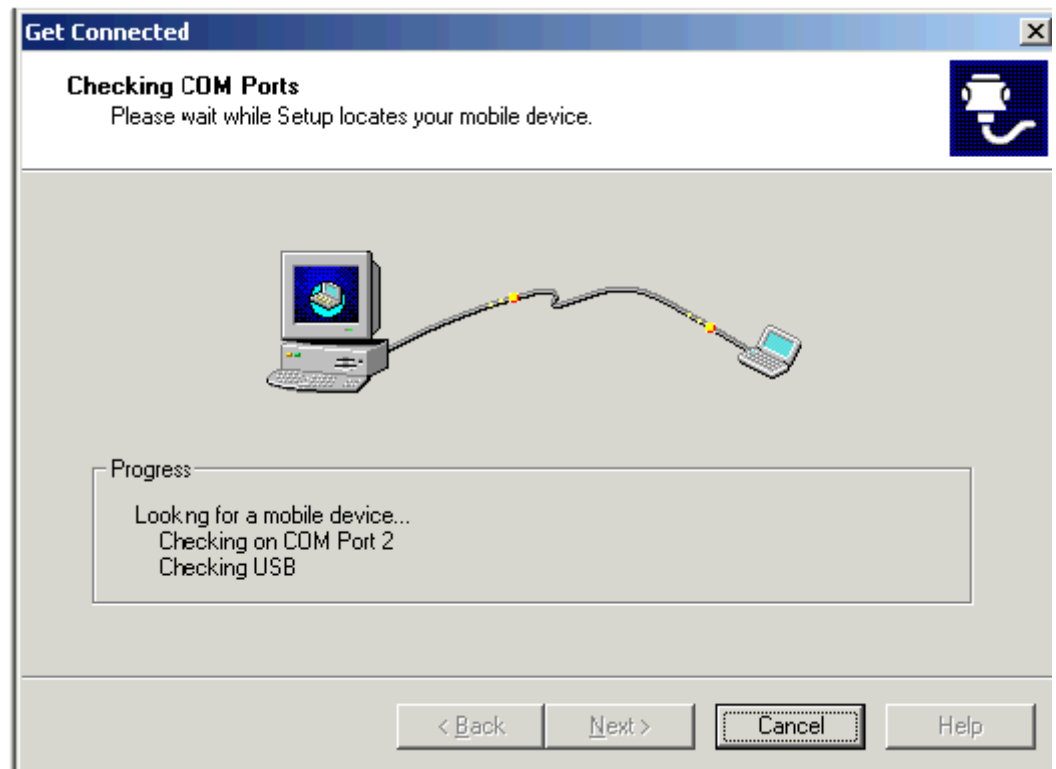
Press **Next** to install Microsoft ActiveSync in the default folder, or **Change** to select another installation folder.



Place the Pocket PC in the docking station and press **Next** to connect to it.

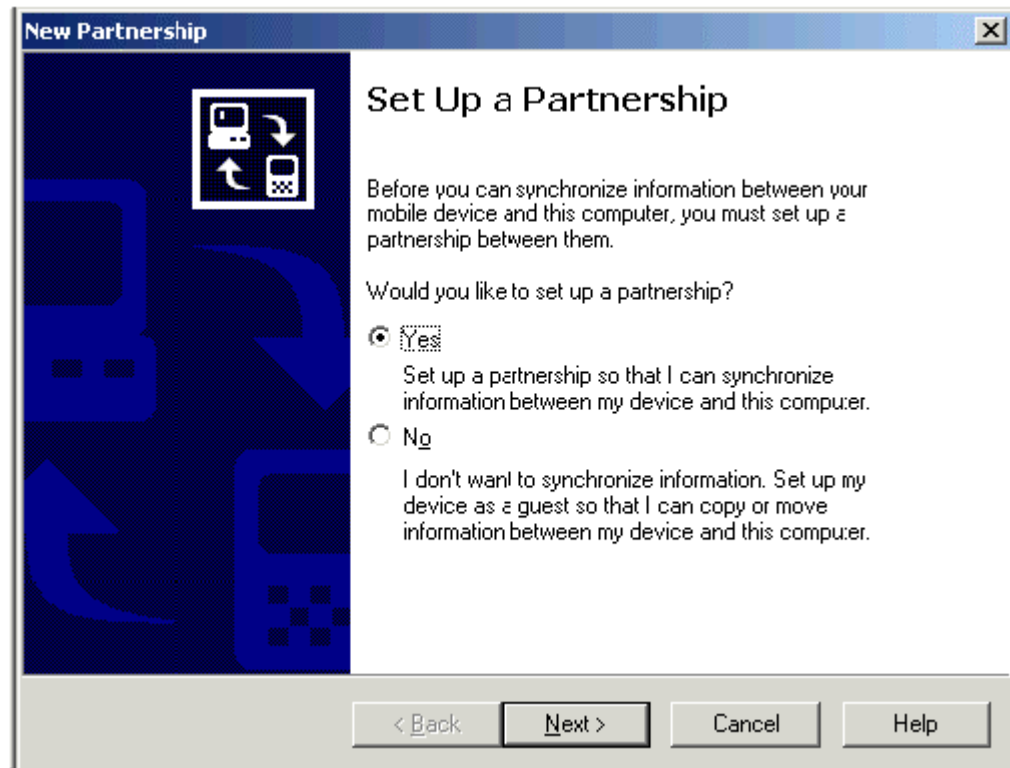


Microsoft ActiveSync will now check all COM ports on different baud rates, and should eventually find the Pocket PC and connect to it.

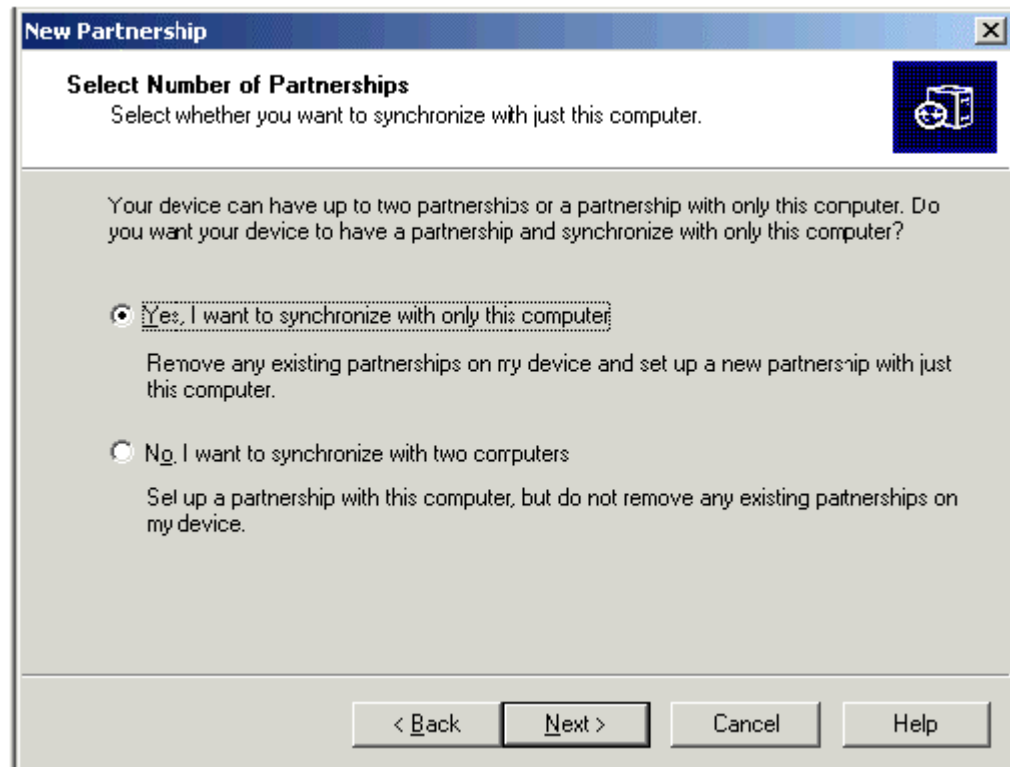


Set up partnership.

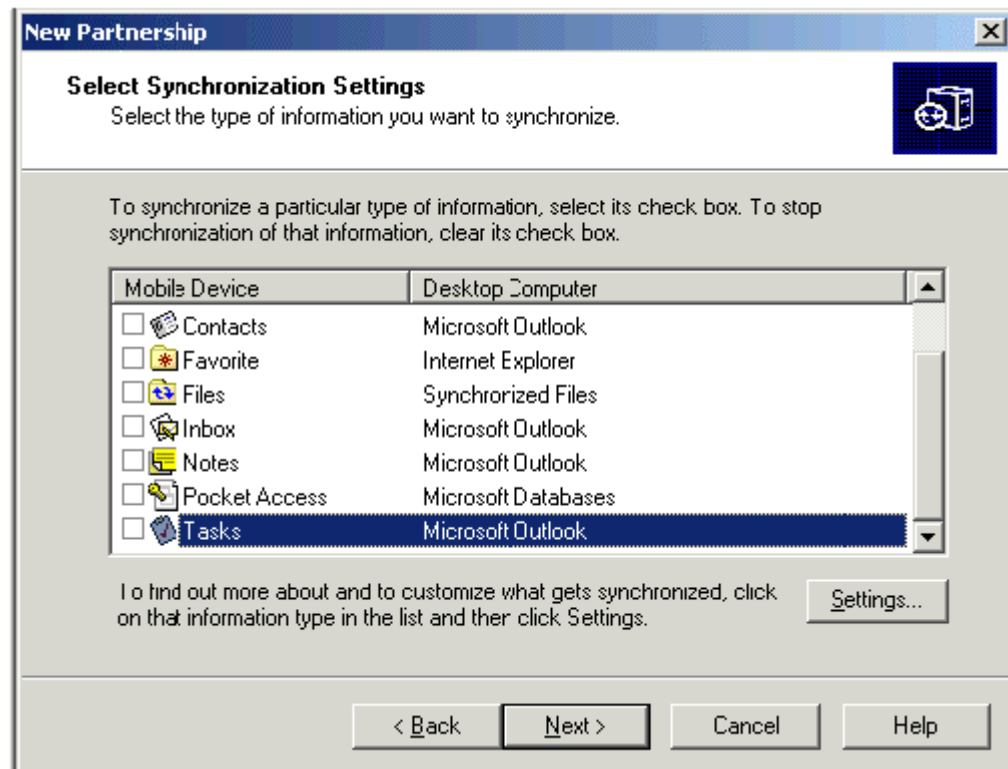
When Microsoft ActiveSync has found the Pocket PC, it asks to set up a partnership. Select **Yes** and continue by pressing **Next**.



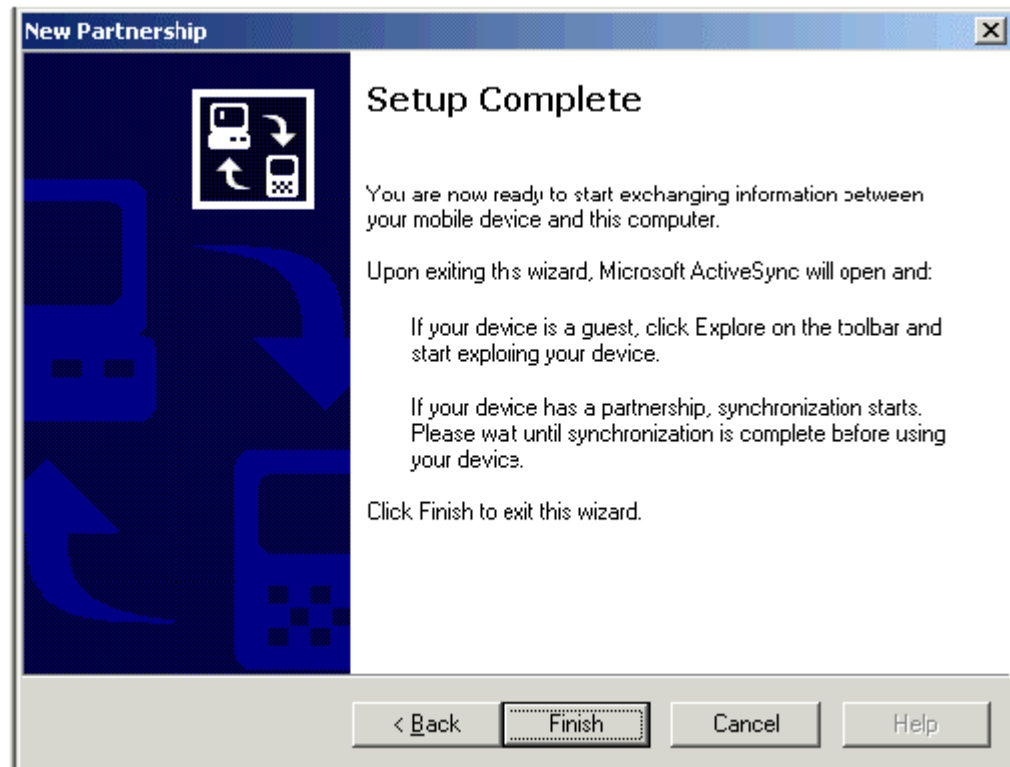
In the next dialog, select “Yes, I want to synchronize with only this computer.” Continue by pressing **Next**.



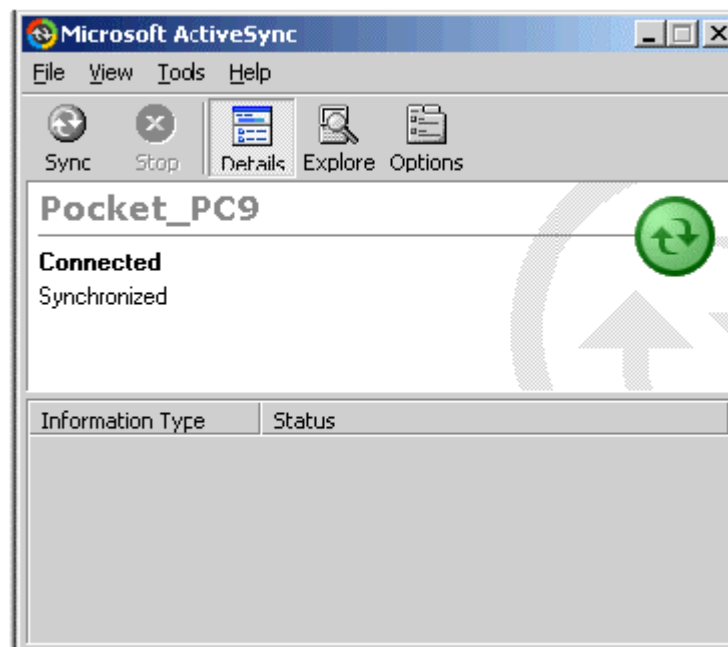
In the Select Synchronization Settings dialog, **deselect** all items in the list before continuing with **Next**.



The Setup Complete dialog indicates that the partnership is set up. Press **Finish**.

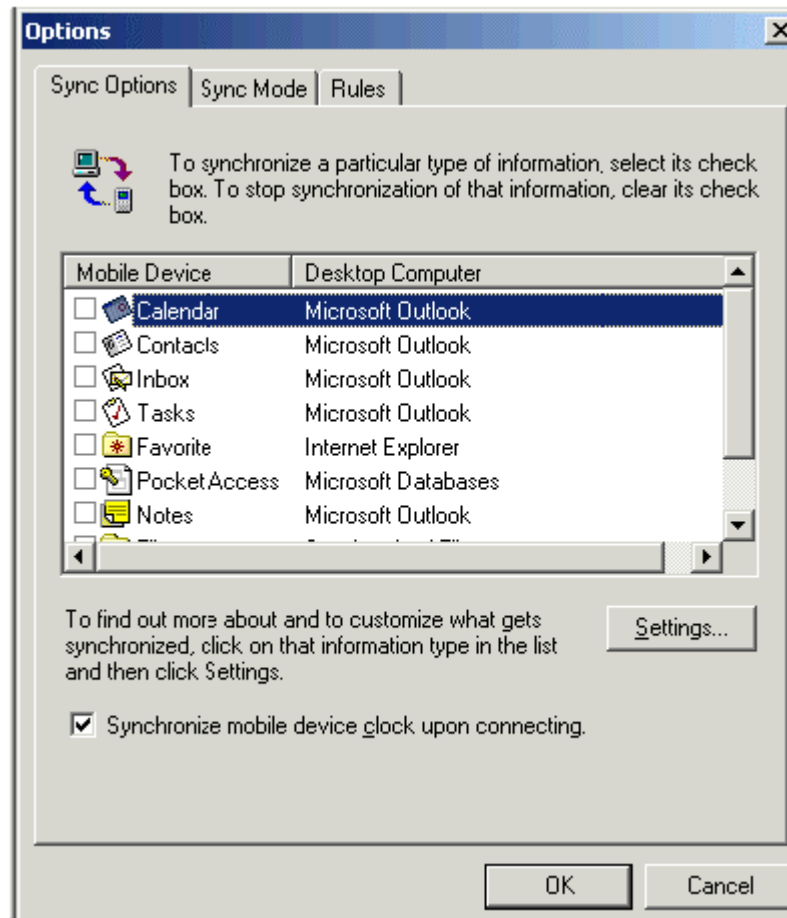


The following window indicates that the Pocket PC is connected and synchronized.



The green round symbol in the system tray (as above) indicates connection.

Press **Options** in the Microsoft ActiveSync window, and check the option “Synchronize mobile device clock upon connection.” Press **OK**. The installation of Microsoft ActiveSync is now complete.



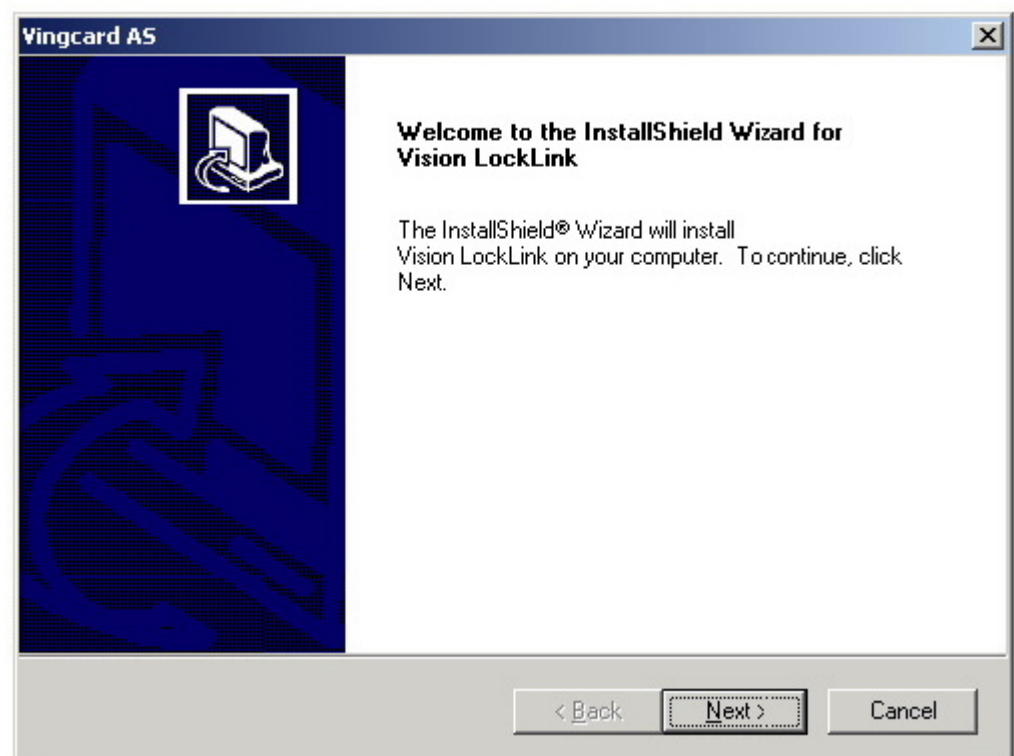
Installing Vision LockLink

Locate the Vision LockLink setup files on the VingCard Locklink CD, and run the desktop installation program `setup.exe`.

If LockLink is to be installed from Compact Flash card, insert the card, and jump to step 7.

NOTE: Installing the LockLink from the desktop requires that the Pocket PC is connected to the PC.

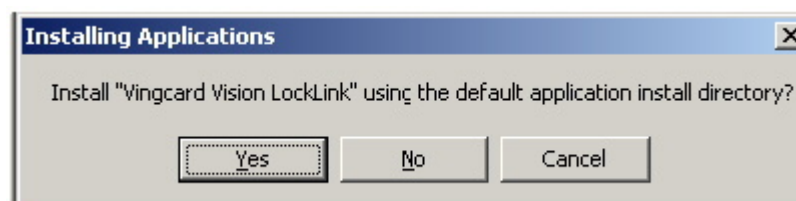
Follow the onscreen instructions and press **Next**.



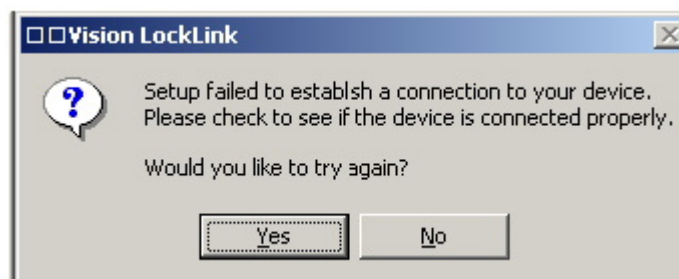
Select the type of the Pocket PC and press **Next** to continue.

Note that LockLink v2.0 supports only the StrongArm processor as specified for PocketPC 2002 running Windows CE 3.0 or later. Example device : Compaq iPaq.

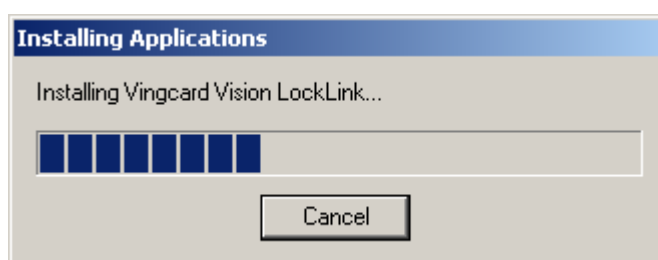
Answer **Yes** when asked to install into the default directory.



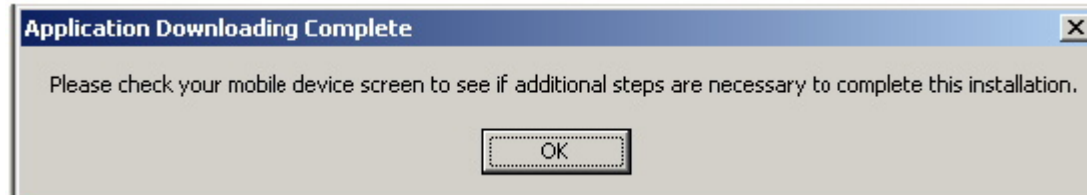
If no connection to the Pocket PC is established (with Microsoft ActiveSync), the following error message appears. In this case, place the Pocket PC back into the docking station, and wait until the connection is established. Press **Yes** to try again.



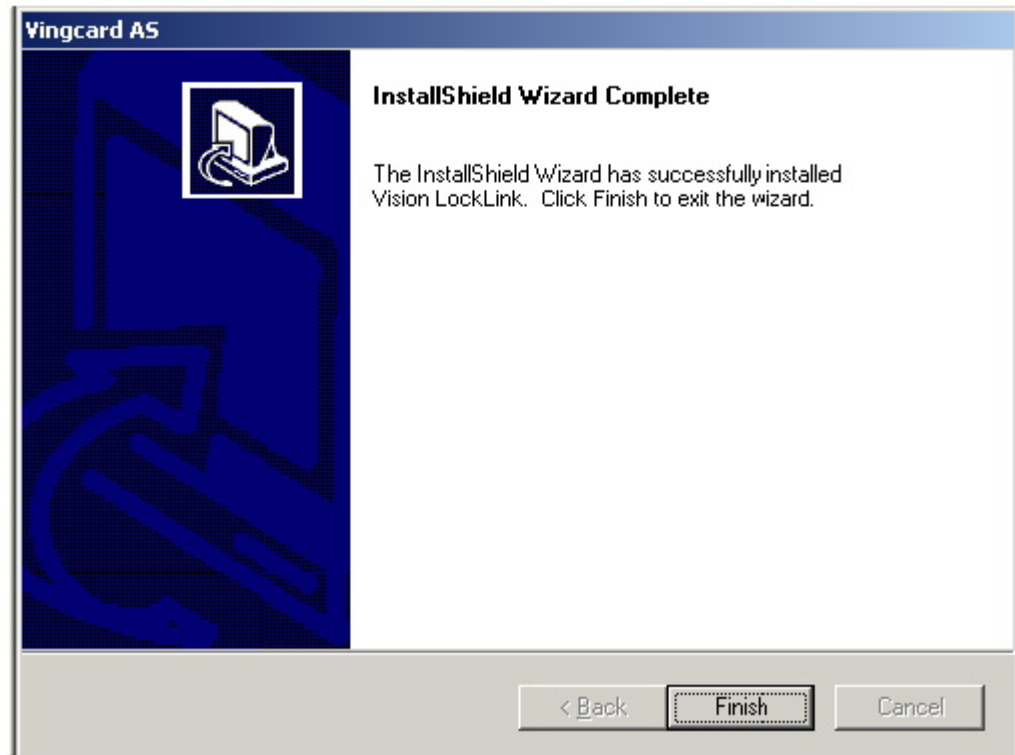
The Vision LockLink files are now being installed. Note that this may take some minutes to complete. The installation indicator shows the progress of the installation.



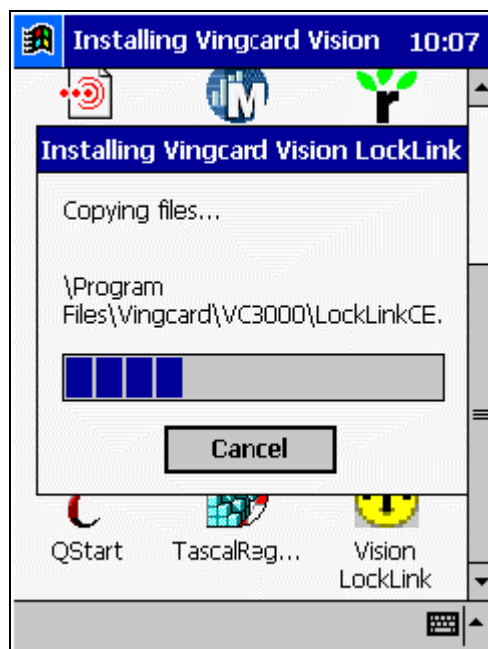
The installation on the workstation is finished. Press **OK**.



Press **Finish** and continue installation on the Pocket PC.

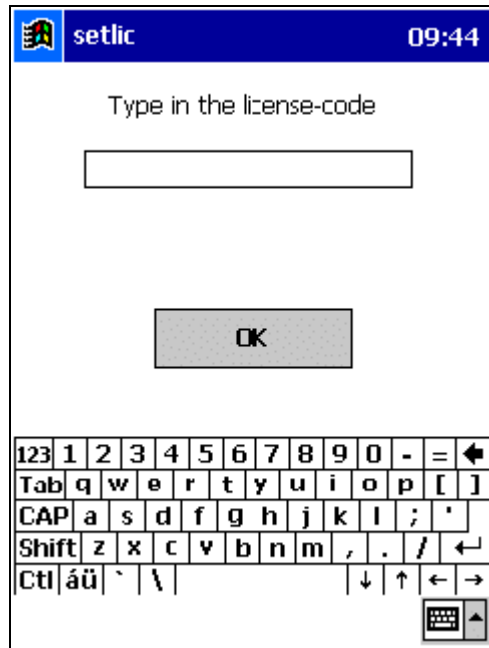


The installation is running on the Pocket PC as shown in the figure below.



Type in the license code provided with Vision LockLink. To open a keyboard, press the keyboard icon in the taskbar. When you have typed in the license code, press **OK**.

The license code 'demo' will work for demo installations.



setlic 09:44

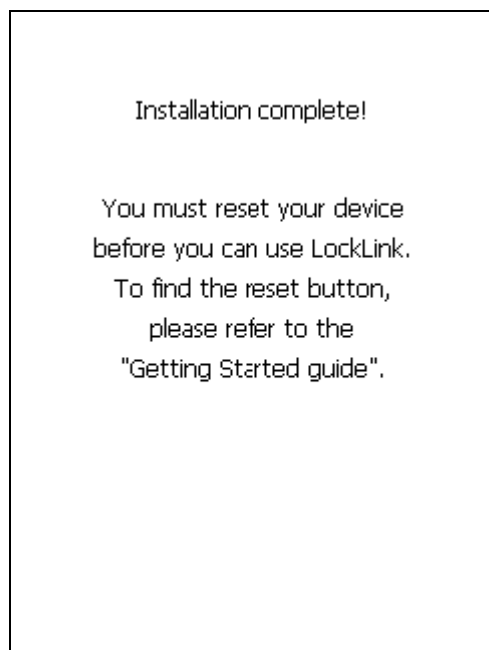
Type in the license-code

OK

123	1	2	3	4	5	6	7	8	9	0	-	=	↵
Tab	q	w	e	r	t	y	u	i	o	p	[]	
CAP	a	s	d	f	g	h	j	k	l	;	'		
Shift	z	x	c	v	b	n	m	,	.	/		↵	
Ctl	á	ü	`	\								↓	↑

Keyboard icon in taskbar

Reset the Pocket PC. Note that the Pocket PC must be reset before the Vision LockLink can be used.



Installation complete!

You must reset your device
before you can use LockLink.
To find the reset button,
please refer to the
"Getting Started guide".

Resetting is done by pressing the small recessed button at the Pocket PC. Refer to the manual for your specific Pocket PC model for details of exactly where to find it.

On Compaq Aero PPCs it is located on the back of the device.

On Compaq iPaqs it is located on the underside (the edge that sits in the cradle).

After resetting, go to the PC Connections screen (**Start/Settings/Connections/PC**) and make sure the 'Automatically connect...' checkbox is checked. *When this is checked, the fastest way to establish an ActiveSync connection to the PC is to turn the Pocket PC off, then immediately on again.*

Go to **Start/Settings/Buttons** and note the button settings for the Pocket PC. All those labelled VLaunchx or Vision LockLink will launch Vision LockLink. You can change the settings if you wish (via the Button Assignment drop down control) to match your own preferences. For example, you might allocate one button to <Start Menu>.

Start the Vision LockLink. You can start it by pressing **Start/Programs/Vision LockLink**, or by pressing any of the buttons assigned to launch LockLink (see previous step).

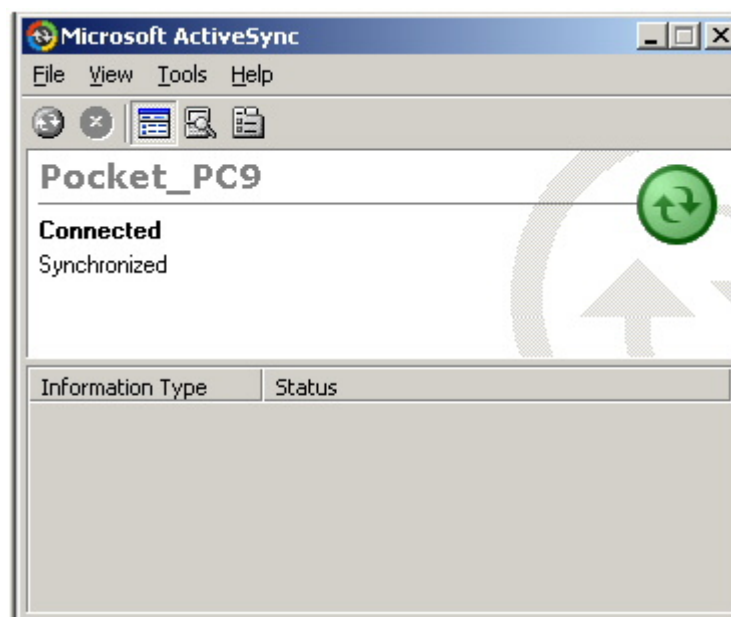
Before the LockLink can be used, you must download the lock programs and lock data as described in the next section.

Loading lock data from Vision workstation

Individual lock data for each lock is created by the Vision application, based on the property specific setup stored in the Vision database. Any PC connected to the Vision network can access the database and build the lock data.

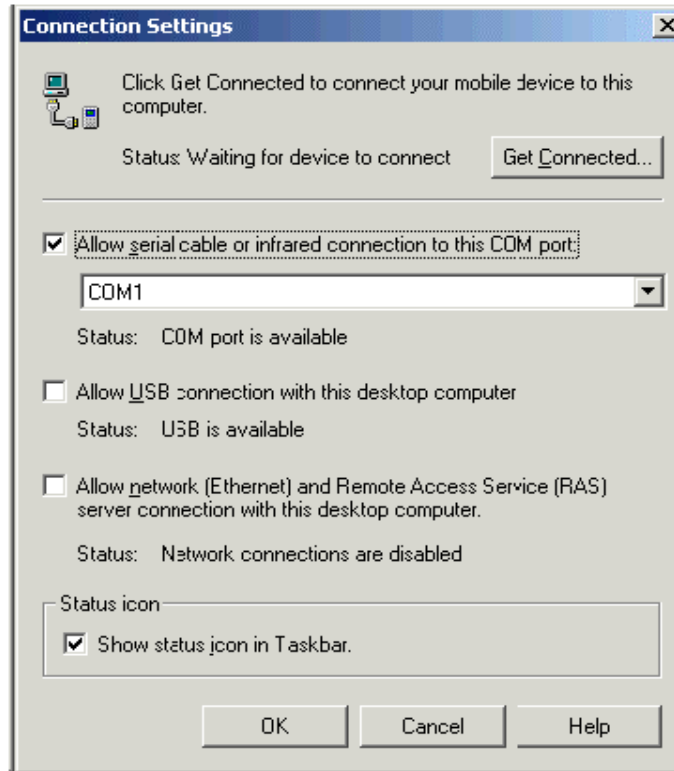
To program the locks, the lock data must be transferred from a PC running Vision (and ActiveSync) to the LockLink Pocket PC.

1. Make sure the docking station is connected to the Vision PC and the Pocket PC is turned on and is in the docking station.
2. In the Vision PC, check that ActiveSync is running and that the Pocket PC is connected and synchronised.



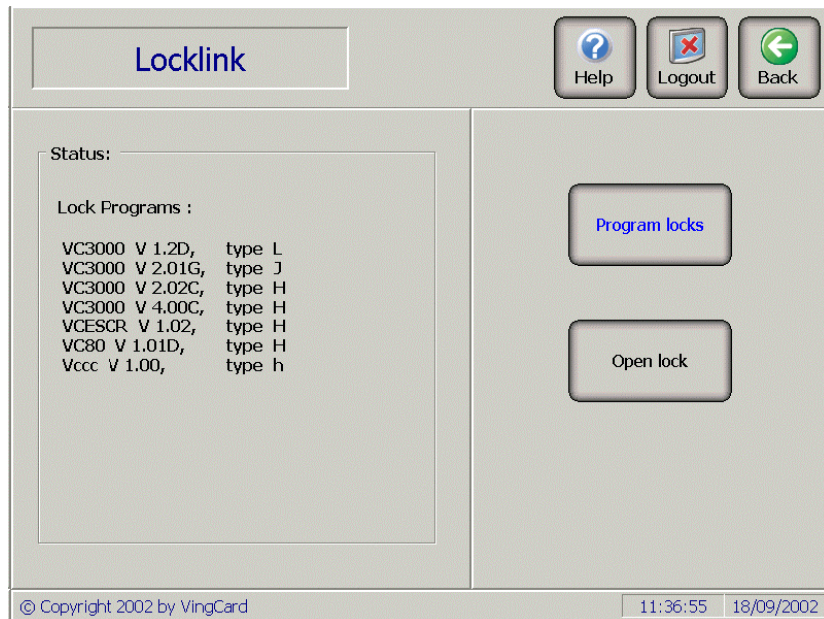
3. If it isn't, connect and synchronise either by
turning the Pocket PC off then immediately back on OR
logging in to Vision LockLink on the Pocket PC and pressing the **Dock** button

If you still cannot connect, check the ActiveSync connection settings. In particular, check that ActiveSync is allowed to use the com port the Pocket PC is connected to (Com1 in the example below).



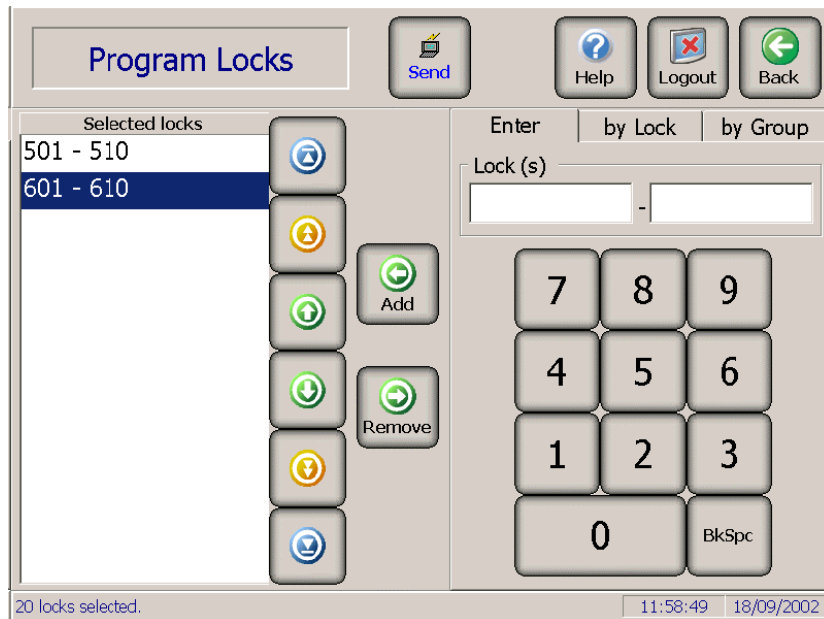
4. On the Vision PC main screen, start Vision, login and press the **LockLink** button to start the LockLink module.

Press **Program Locks**.

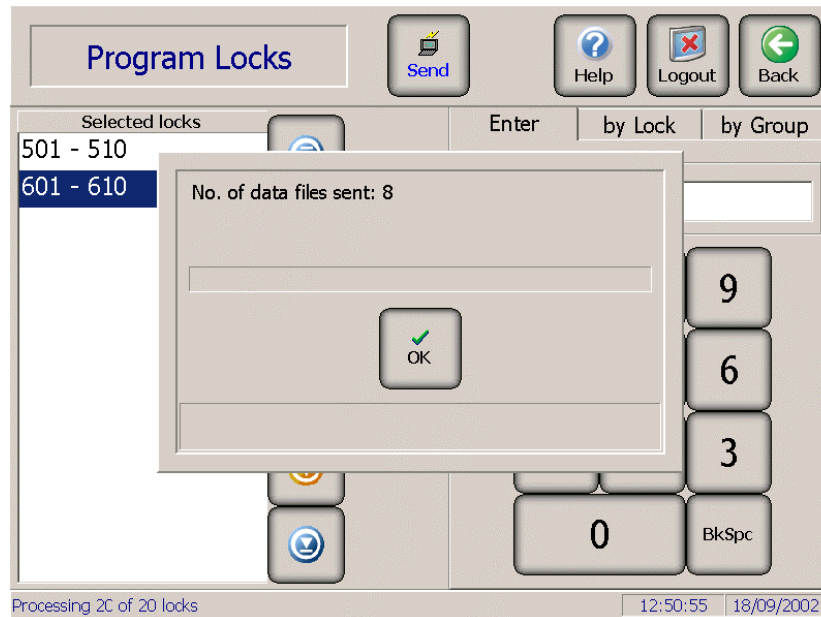


5. In the Program Locks screen, select the locks to be programmed and press **Send**.

You can specify the locks by using the number pad or by selecting individual locks or lock groups.



6. The lock data is built and downloaded to the Vision LockLink. Press **OK** on completion



Starting the LockLink



Vision LockLink can be started several ways. The shortcut-icon can be tapped on the Pocket PC, and is also found in “**Start->Programs**”. The buttons on the Pocket PC are also assigned by default to start Vision LockLink – although you may change the button settings, see the last step of “Installing Vision LockLink” earlier in this Chapter.

If the VingCard **DA VINCI LockLink** software-product is also installed it will be assigned by default to button number 1. If the **ELSAFE SafeLink** software-product is also installed it will be assigned by default to button number 4. You can only run one LockLink application at once. If either of these applications is running, all LockLink assigned buttons on the Pocket PC will bring the running application to the front rather than launch the new application. The running application must be quit first. LockLink and SafeLink can be run simultaneously, but we recommend against it (possible com port conflicts).

A password screen will appear when Vision LockLink is started. It will present a number keypad if your Vision system is configured for numeric only PIN code style passwords, or an alphanumeric keypad if the system is configured for Username and Password. Both password screens are shown below.

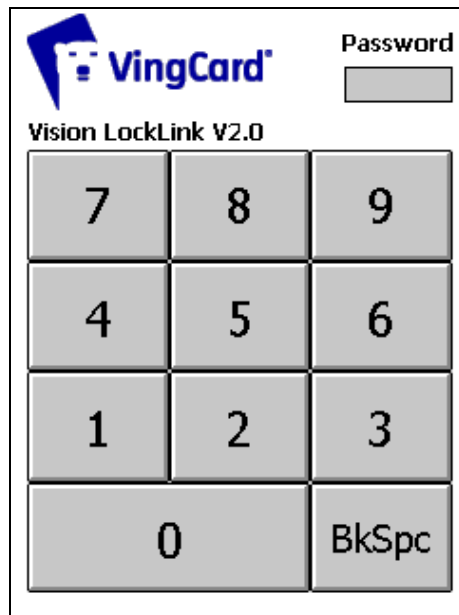
For the Alphanumeric keypad only:

- To enter numbers from the alphanumeric keypad, press the “123” button then select the required number. To re-show letters, press “ABC”.
- You may still enter a numeric only PIN code style password in the Password box-without a username.
- You must press **Enter** after entering your password

- Username is not case sensitive but password is. Use the **CAPS** button as required.

If no data is uploaded to the LockLink, the **BkSpc** button will be replaced with the **Dock** button. This can be used to establish an ActiveSync connection to the Vision PC.

Note that if the Pocket PC is switched off when Vision LockLink is running, and then turned on again, Vision LockLink will log out automatically, and the password screen will appear again.



The image shows the 'Password' screen of the VingCard Vision LockLink V2.0. At the top left is the VingCard logo. To its right is the text 'Password' above a small rectangular input field. Below the logo and input field is the text 'Vision LockLink V2.0'. The main part of the screen is a numeric keypad with buttons for digits 0 through 9. The '0' button is wider than the others. To the right of the '0' button is a button labeled 'BkSpc'.

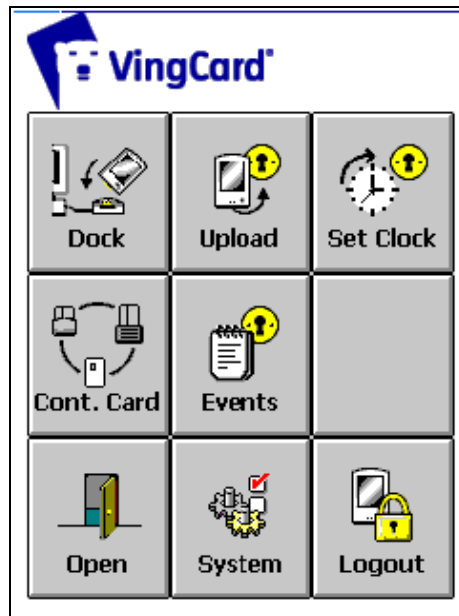


The image shows the 'Username' screen of the VingCard Vision LockLink V2.0. At the top left is the VingCard logo. To its right is the text 'Username' above a small rectangular input field. Below the logo and input field is the text 'Vision LockLink V2.0'. The main part of the screen is an alphanumeric keypad. It has a 4x4 grid of buttons labeled with letters A through Z. The 'BkSpc' button is located at the bottom right of the grid. To the right of the grid is a vertical column of buttons: '123', 'CAPS', and 'Enter'.

LockLink functions

The following figure shows the basic functions of the LockLink that will be explained in more detail in the following sections.

All the step instructions in this chapter begin from the LockLink main menu if not stated otherwise. It is thus assumed that you have logged in to the LockLink.



NOTE: After three minutes of inactivity, the user will be logged out and the Pocket PC will be automatically turned off.

Docking the LockLink Pocket PC

The LockLink Pocket PC is connected to a Vision PC via the docking station.

1. Place the Pocket PC in the docking station. The Vision PC and the Pocket PC should establish a connection via ActiveSync. If they don't, connect and synchronise either by
 - turning the Pocket PC off then immediately back on
start>settings>connections>PC>Automatically synchronize... should be checked on
 - OR
 - logging in to Vision LockLink on the Pocket PC and pressing the **Dock** button

Programming locks

When programming locks, you can upload either the lock program and lock data or only the lock data. Uploading the lock program is slower than uploading only the lock data.

Upload both the lock program and the lock data if

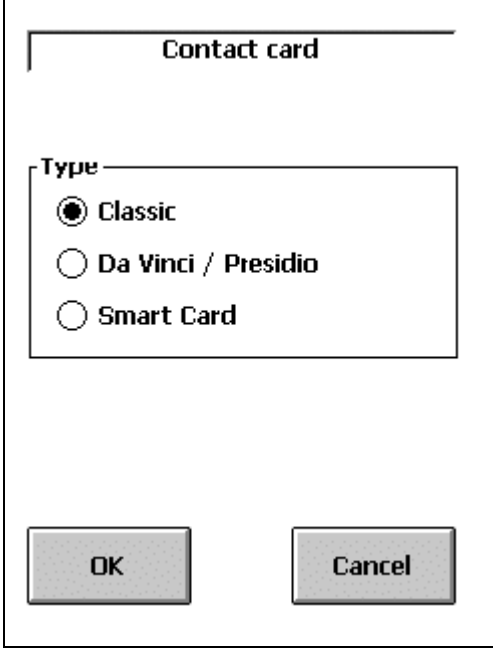
- you are programming a new lock,
- you want to upgrade the lock program,
- you have changed the batteries of the lock, and the lock has been without power for more than three minutes, or
- the lock batteries were completely discharged,

Upload only the lock data if the Vision system configuration has been changed.

Uploading program and data to locks

1. Check that the LockLink is set to the correct time, as it will automatically be used to set the time in the lock.

2. Check that the Contact Card is attached to the Pocket PC. Select the **Cont. Card** button from the main menu and then select the appropriate Contact Card setting for the lock you are about to upload to. Press **OK** to return to main menu.



Contact card

Type

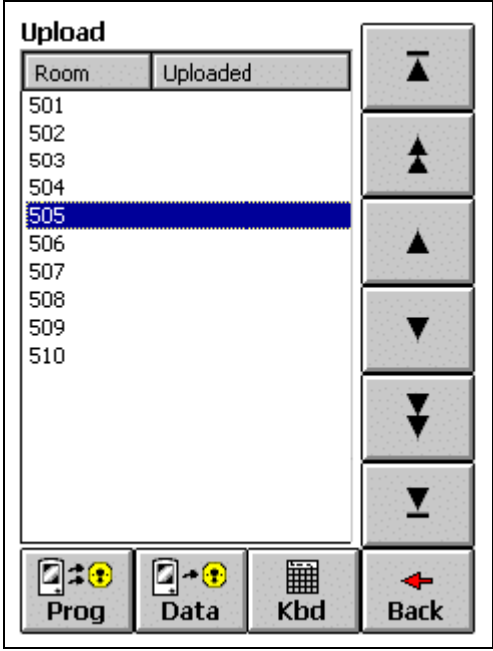
☒ Classic

☐ Da Vinci / Presidio

☐ Smart Card

OK Cancel

3. Press the **Upload** button. In the Upload screen, select the lock to be programmed. If necessary, use the arrow buttons to scroll the display.



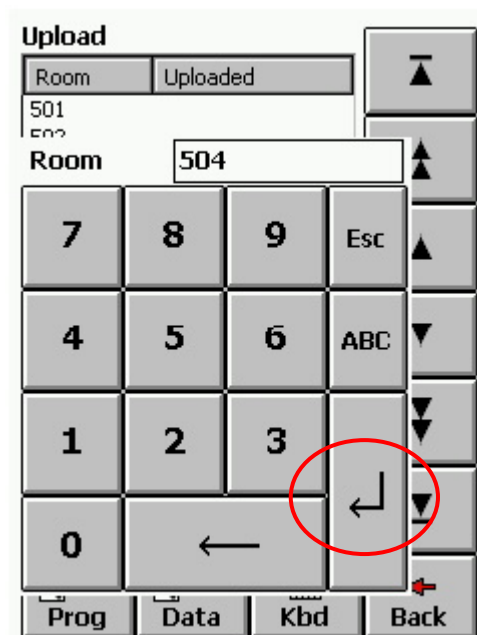
Upload

Room	Uploaded
501	
502	
503	
504	
505	
506	
507	
508	
509	
510	

▲ ▲▲ ▼ ▼▼ ▼

Prog Data Kbd Back

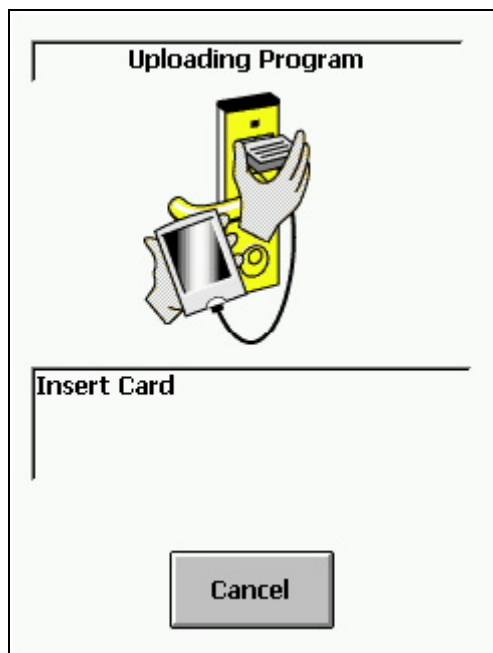
If you want to use a keyboard to insert the room number instead of scrolling the list, press **Kbd**. The following screen appears. Type in the room number. If the room number contains letters, press **ABC** to display the letter keypad. Press the Enter key to return to the room list with the typed number selected.



4. To upload the lock program and lock data, press **Prog**.

To upload only the lock data, press **Data**.

5. Follow the instructions given on the display. For example :



Finally, press OK to complete the operation.

NOTE: For a new Vision installation, all locks must be programmed using the **Prog** button.

Reading events

A detailed, time ordered list of lock events can be transferred from each VingCard lock to the LockLink. The events can then be viewed on the LockLink or transferred to a Vision PC for viewing and / or printing.

Lock events are with the Contact Card appropriate for the lock. In addition, for locks that accept Smartcards, a special Read-out keycard can be used to read and transfer lock events. For detailed information on using the Read-out keycard, see Chapter 6.

What the read-out contains

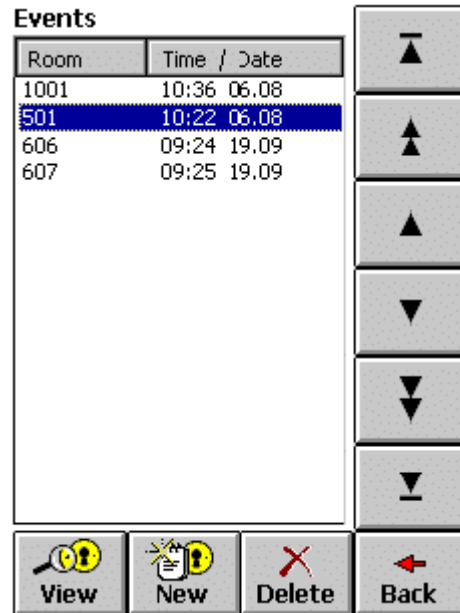
The read-out contains the following information:

- The room number. The LockLink automatically detects the room number at the read-out.
 - Standard lockset (lock controller) or Remote controller events.
 - Details about when the lock was opened and closed and whether unsuccessful attempts were made to open the lock (unsuccessful attempts can be omitted from the lock read-out by changing the lock parameters in **Vision > Setup > Locks > Lock Groups**).
 - The time and date of the occurrence
 - 1 minute resolution for all Da Vinci, Presidio and Smartcard locks
 - 1 minute resolution for newer VC3000 locks (Halifax 32k)
 - 5 minute resolution for older VC3000 locks (Halifax 8k, LCU, Jackpot)
 - Information about the keycard that was used in the lock (User Type, User Group, whether keycard was valid, invalid or new (first time used in lock), the User ID, Override criteria etc.
-

NOTE: If you transfer the information to the Vision PC and print it, the User Name will be included.

Downloading events from a lock

1. Press **Events** on the LockLink main menu.
2. On the Events screen, press **New**.



3. Follow the instructions on the screen.

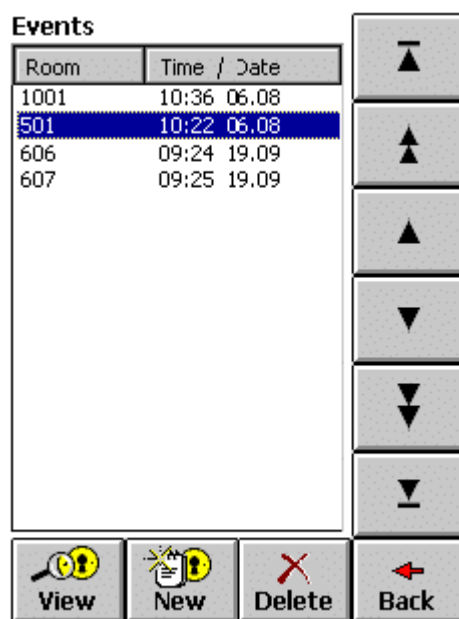
Note that you cannot specify the lock number in LockLink before downloading the events. The lock number is read from the lock during the download.

When the download is finished, the room will be added to the room list in the Events screen. If you download information on a room that already exists on the list, LockLink will ask if you want to override the existing entry.

Viewing downloaded events

After you have downloaded events from a lock to the LockLink, you can view the results:

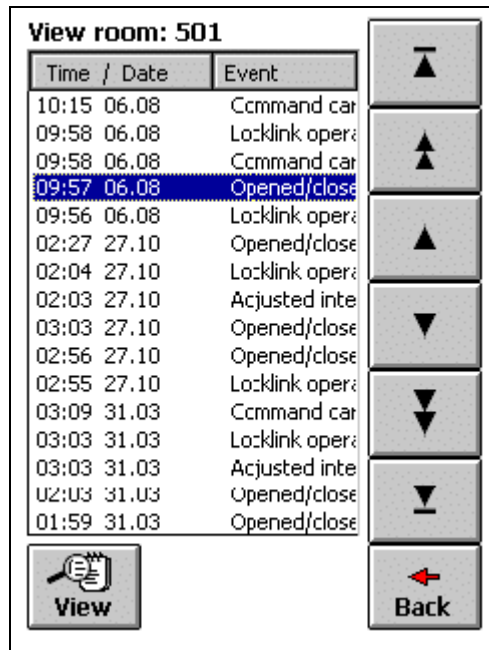
1. If you are not already at the Events screen, press **Events** on the LockLink main menu to display the Events screen.
2. Select the room that you want to view events from and then press **View** to display the View room screen. If necessary, use the arrow buttons to scroll the display. To go back to the main screen, press **Back**.



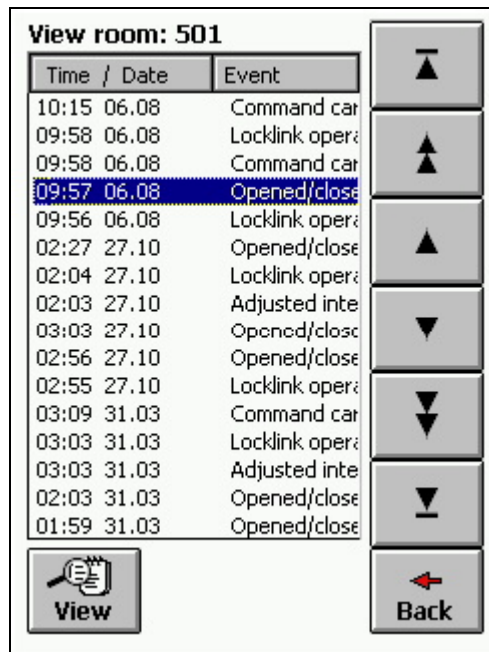
To delete the events of the selected room, press **Delete**.

3. You will be presented with a list of events. Use the navigation controls to select the event you want to view in more detail and press **View**.

To go back to the main Event screen, press **Back**.



4. When viewing event details, if you want to view previous (later in time) or next (earlier in time) events, press Prev or Next. To go back to the Event List screen, press Back.



5. You can transfer the downloaded events to the Vision PC for viewing and printing using the Vision Reports module. For detailed information, see the Reports section in Chapter 5.

Unlocking doors with the LockLink

The LockLink can be used to open doors. It uses its own battery to open locks in situations where the lock battery does not have enough charge left to open the door.

NOTE: Before a lock can be opened with the LockLink, it is necessary to use the Vision LockLink module to give the LockLink instructions naming the *specific* locks you want to open. This is done for security purposes, so that the LockLink cannot open doors without proper authorization.

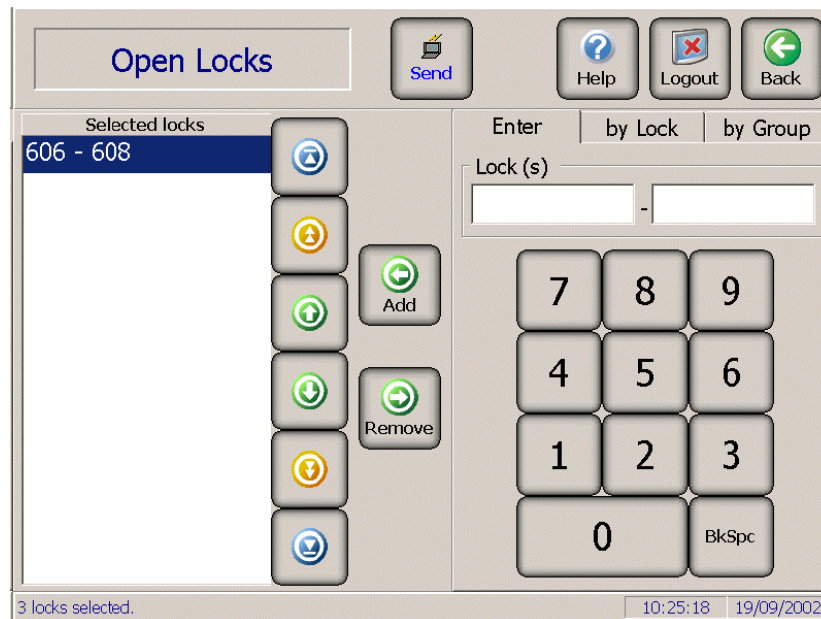
1. Make sure the docking station is connected to the Vision PC and the Pocket PC is turned on and is in the docking station.
2. On the Vision PC, check that ActiveSync is running and that the Pocket PC is connected and synchronised. (*for more detail, see earlier section on transferring lock data to LockLink*).
3. On the Vision PC main screen, start Vision, login and press the **LockLink** button to start the LockLink module.

Press **Open Lock**.

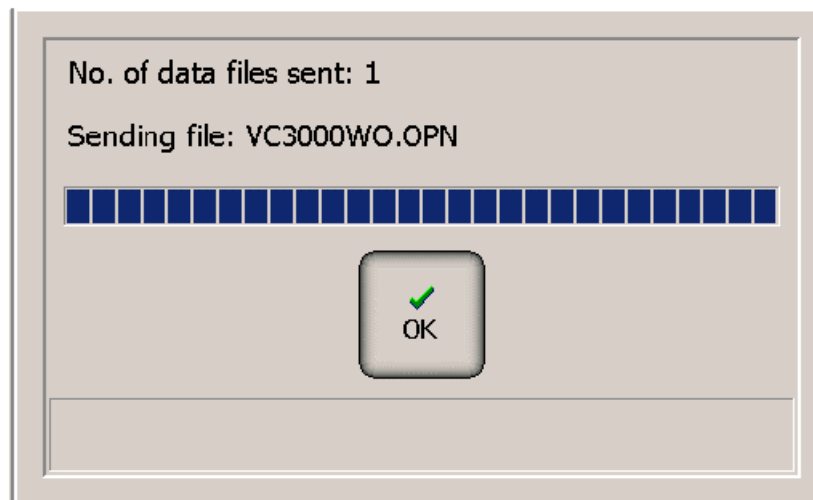


4. In the Open Locks screen, select the locks to be opened and press **Send**. You may select up to 10 locks at once. Refer to the information message at the bottom left of screen.

You can specify the locks by using the number pad or by selecting individual locks or lock groups.

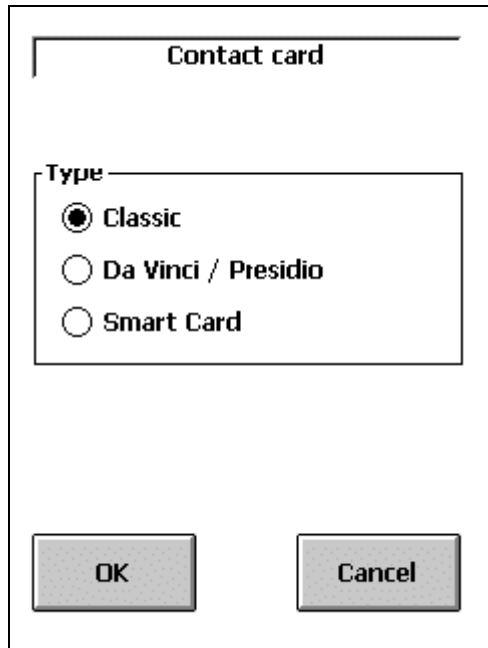


5. The open lock data is built and downloaded to the Vision LockLink. Press **OK** on completion



The data necessary to open the specified doors is now on the LockLink. It is only valid for 1 hour

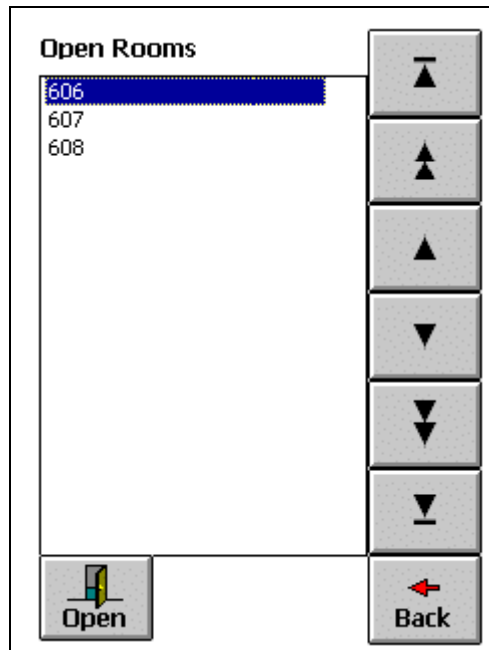
6. Go to the door you want to open and connect the **Contact Card** to the LockLink Pocket PC. Select the Cont. Card button from the main menu and then select the appropriate Contact Card setting for the lock you are about to open. Press OK to return to main menu.



The screenshot shows a 'Contact card' dialog box. The title bar reads 'Contact card'. Below the title bar, there is a section labeled 'Type' which contains three radio button options: 'Classic' (which is selected), 'Da Vinci / Presidio', and 'Smart Card'. At the bottom of the dialog box, there are two buttons: 'OK' and 'Cancel'.

7. Press **Open** on the main menu of the LockLink.

8. Select the room you wish to open. Press **Open** and follow the instructions on screen.



Note that the Da Vinci style contact card has a built in battery and so can open 'dead' locks as well as those that still have their own battery power.

When using the Classic or Smartcard contact card, you should first attempt to open the lock just using the contact card. If this does not work, the lock battery is probably dead. In this case, attach the external battery unit to the contact card and try again.



The Open Lock authorization is valid for 1 hour only.

Setting the Daylight Saving Time in the locks

In order for the time of Lock Events to be correctly reported, each lock needs to be updated with the correct Daylight Savings Time (DST) information – that is, the dates and times that DST starts and finishes for the current year.

For locks where Smartcards are used regularly – this includes non-processor, memory cards - the Daylight Saving Time information in the lock is updated automatically. DST information is written to each Smartcard produced, and when these are used in the lock they transfer the information to the lock. Thus the lock will always have up to date DST information and will therefore be able to correctly adjust its internal clock .

For locks where Smartcards are NOT used regularly – this can either mean locks that cannot read Smartcards or locks where Smartcards are not used often – the DST start and end information is not carried to the locks by keycard and therefore should be transferred to each lock once a year using the LockLink. For example, this could be done in January, when Windows has made the new settings for the year available to Vision. Then, when the DST changes occur (for example in April and October) the lock will have the up to date DST information necessary to correctly adjust its internal clock .

To carry out the yearly update of DST information to 'non Smartcard' locks :

- Make sure DST is activated and correct in Vision > Setup > System parameters > Daylight Savings.
- Transfer some lock data from Vision to LockLink. See earlier step by step guide. This ensures that the DST dates/times are transferred to LockLink.
- Use the LockLink on all the locks by pressing **Set clock** from the main menu and follow the instructions on the display. As well as synchronising the Pocket PC and lock clocks, this transfers the updated DST information to the lock.

The locks will then automatically change at the correct point in time.



The time is rounded to the next 1 minute interval. This is done for security purposes so that you will know if an attempt to enter a room was made multiple times within a short time frame.

Recording LockLink log

The Vision LockLink allows you to record a log on the LockLink containing information that can be used for troubleshooting. Note that this will slow down the LockLink operation.

1. On the LockLink main menu, press **System**.
2. Check the “Log to file” option and press **OK**. This starts recording the log. The log is stored as ‘debug’ in Pocket PC folder Program Files\VingCard\VC3000\Log. It can be transferred back to the PC using ActiveSync for viewing.

Exiting LockLink

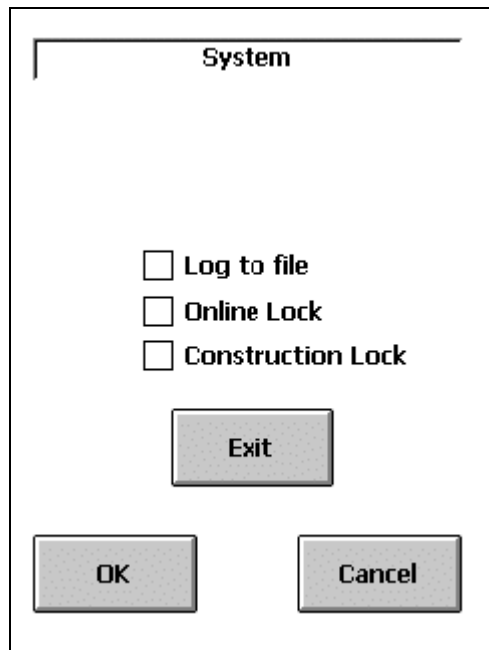
Normally you do not need to exit the LockLink software. The recommended way to close the LockLink software is to turn the Pocket PC off by pressing the Power Off button. When you turn the Pocket PC on, the login screen is displayed.

To return to the login screen from the LockLink program, press **Logout** on the main menu. After that the LockLink software is accessible only with a valid password.

In practise, exiting the program is only necessary when updating the LockLink program to a newer version. To exit the LockLink software, do the following:

1. On the LockLink main menu, press **System**.

2. In the System screen, press **Exit**.



3. Now press **Yes** to exit.

Chapter 5 : Using Vision Modules

How to Exit the Vision System

Click the **Back** button to return to the **Main** menu.



Click the **Exit** button.



NOTE: If the Exit button does not appear on the Main menu, you are required to have access to the System Setup Module to exit the system.

If you have access to the Setup module, you can choose to have the Exit button displayed on the Main menu (Setup > System Parameters > General > Exit Button). This setting will apply to all users.

Main Menu of VISION Modules





















Each user has access to any modules that do not appear greyed out in the **Main** menu:

Option	Description
Guest Keycards	Check in guests, make duplicate keycards, change check out dates, check out guests, replace lost or stolen keycards, determine to which room a keycard is assigned.
Reports	View or print reports on system events, lock events, employees, or the current setup.
System Setup	Set System Parameters that control the Vision system and create System Access Groups and password levels for employees who need to use Vision. This module also allows you to Exit the Vision system.
Employee Keycards	Create keycards for employees based on User Groups set up for your hotel.
Employee Rooms	Check employees into rooms with all of the functionality and features of the Guest Keycards module.
Backup	Backup and restore Vision system data.
Special Keycards	There are options to make keycards that : prevent door access for existing employee and guest keycards; set a door to remain unlocked (Passage Mode); download data or diagnostic information from locks. You can also create keycards that can be used to check in guests if the computer system ever goes down.
System Users	Set up employee access to Vision modules based on User

	Access Groups set up by your hotel.
LockLink	Accesses LockLink Pocket PCs, which relay information between locks and the computer system.

Symbols and Buttons

The following is an explanation of what the most commonly used buttons in the Vision system do.

	Appears on the numeric and large on-screen keyboards. Erases one character at a time.		Moves to the top of the displayed list.
	Moves back one month in the calendar.		Moves to the bottom of the displayed list.
	Moves forward one month in the calendar.		Moves one screen upward on the displayed list.
	Moves the selected item to the list on the left.		Moves one screen downward on the displayed list.
	Moves the selected item to the list on the right.		Moves one item upward on the displayed list.
	Moves all of the items to the list on the left.		Moves one item downward on the displayed list.
	Moves all of the items to the list on the right.		Displays an on-screen keyboard.
	Displays Help for the screen that is currently displayed. Select Main menu from within Help for additional topics.		Returns you to the previous screen.
	Logs out the current user and returns to the log-in screen		Exits the Vision system.

How Passwords Work

Using the setup module, Vision system can be set up for any of the following password options :

- A randomly generated **4 digit** 'PIN code' style password for each user
- A randomly generated **6 digit** 'PIN code' style password for each user
- A self defined **username and password** combination for each user.

When you enter your password on the Log-in screen, it identifies you to the Vision system.

Your password tells the Vision system:

- Which Vision modules to give you access to—Any modules your password does not have access to will appear "greyed-out" on the **Main** menu screen and you will not be able to select them.
- Which Vision module to use as the start up module from the login screen—Your hotel can set up the Vision system to display the **Main** menu, Check In screen, or any other module as the first screen appears after the login screen.
- Who made a keycard—When a keycard is made, the password of the logged-on user tells the Vision system who made the keycard.

For security purposes, the Vision will automatically return to the Log-in screen after a few minutes of inactivity. This is the same as if you selected the **Log Off** button from the **Main** menu. Whenever the **Log In** screen displays, a valid password will be required for access to any of the Vision modules.

NOTE: Because passwords are used to identify you to the Vision system, each person who uses Vision should be assigned their own unique password. It is important to use only your own password and not give your password to others.

How Keycards and Locks Work

Keycards and locks are programmed specifically for each hotel and work together to control access:

- **Keycards** contain information that you have encoded on them
- **Locks** are programmed using the Vision LockLink program on a Pocket PC. Before a door will unlock, the keycard inserted in it must meet all the criteria programmed into the lock.

Life Cycle of a Typical Guest Keycard

This is the "life cycle" of a typical **guest** keycard and what it does:

1. **The guest keycard is created**—Using the Guest Keycards module, you choose a room (or combination of rooms), a User Group (which specifies other parameters for the guest), and the check in and check out date and times. Any information previously contained on this keycard is permanently erased.
2. **The guest uses the keycard**—When a guest keycard is inserted in a guest room door, the door opens if the following conditions are met:
 - This lock is one of the locks this keycard was made for
 - The keycard is not expired based on the current date and time as set in the lock
 - No special instructions have been given to the lock, which prevents access by this keycard. (Some hotels use Lock-out keycards to prevent a guest from returning to a room between the time they check out and the time their keycard expires.)
3. **The guest keycard becomes invalid**—A guest keycard normally becomes invalid in one of these three ways:
 - a new guest is checked into the room—when a lock has been opened by a newer guest keycard, the existing guest keycard is automatically

invalidated
the check out date and time have expired
some hotels use Lock-out keycards as explained in Step 2

Life Cycle of a Typical Employee Keycard

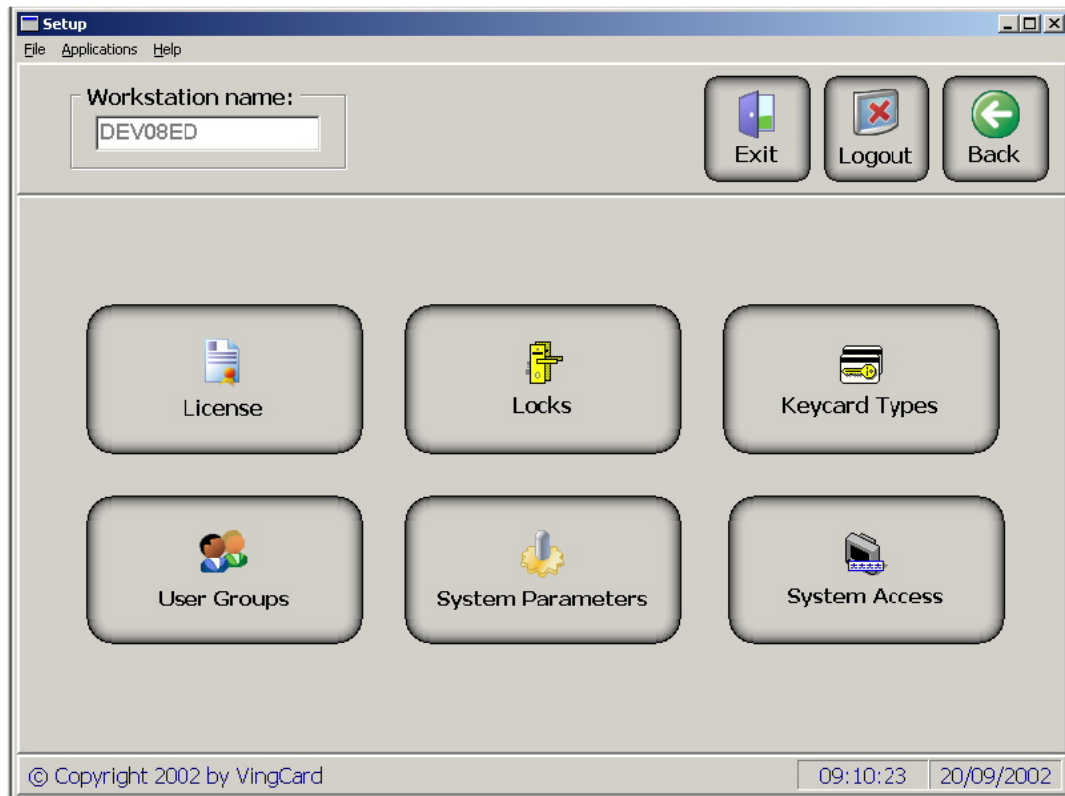
This is the "life cycle" of a typical **employee** keycard made from the Employee Keycards module and what it does:

- 1. The employee keycard is created**—Using the Employee Keycards module, you choose a User Group (which in this case specifies all rooms the employee will have access to) and the name of the person it is assigned to. The keycard is valid for two years. Any information previously contained on this keycard is permanently erased.
- 2. The keycard is used to open doors**—When an employee keycard is inserted in a door, the door opens if the following conditions are met:
 - The User Group on the keycard is valid for this lock. For example, a maid might have access only to guest rooms on a particular floor.
 - The keycard has not expired based on the current date and time as set in the lock
 - No special instructions have been given to the lock by a Void-list keycard, which prevents access by this keycard. This last situation is not very common and hotels normally only use this if an employee keycard is lost or if an employee is no longer employed by the hotel, but has not turned in his employee keycard.
- 3. The employee keycard is replaced or destroyed**
Normally an employee keycard is valid for two years. Before it expires, the hotel makes a replacement keycard. If the employee is terminated, their employee keycard should be destroyed.

System Setup Module

The System Setup module can be run from any PC running Vision : the server or a workstation. The changes you make will affect all workstations using this same Vision database.

System Setup Screen



Option	Description
Setup Menu Bar	The File , Applications , Tools , and Help menu items can be used to access <i>any</i> function of this module.
Workstation name:	This workstation name is always displayed at the top of the screen to indicate which Vision workstation you are on.
Standard Buttons	Exit, Logout, Back
Setup Buttons (main part of window)	<p>These buttons allow you to quickly start any function with just once click of the mouse. The following buttons are provided :</p> <p>License button Use this to enter a new maximum number of locks code. The code can be obtained from VingCard.</p> <p>Locks button Use this to launch the Locks Wizard.</p> <p>Keycard Types button Use this to launch the Keycard Types Wizard.</p> <p>User Groups button Use this to launch the User Group Wizard.</p> <p>System Parameters button</p>

	Use this to set defaults and options for the Vision system. System Access button Use this to control user access to the Vision modules.
--	--

Vision License Settings

Vision License

Current data

Product: DEMO

EV/ES number: DEMO

Facility code: DEMO

Limits

Locks: 2000 Time Tables: 8

User Groups: 256 Common Doors: 53

New code entry

OK Apply Cancel Help

Your current licensing information will appear on this screen. There will be a maximum number of locks, time tables, user groups and Common Doors allowed.

You can use this screen to upgrade your license limits.

If you wish to upgrade your license limits, please contact VingCard or your Vision representative.

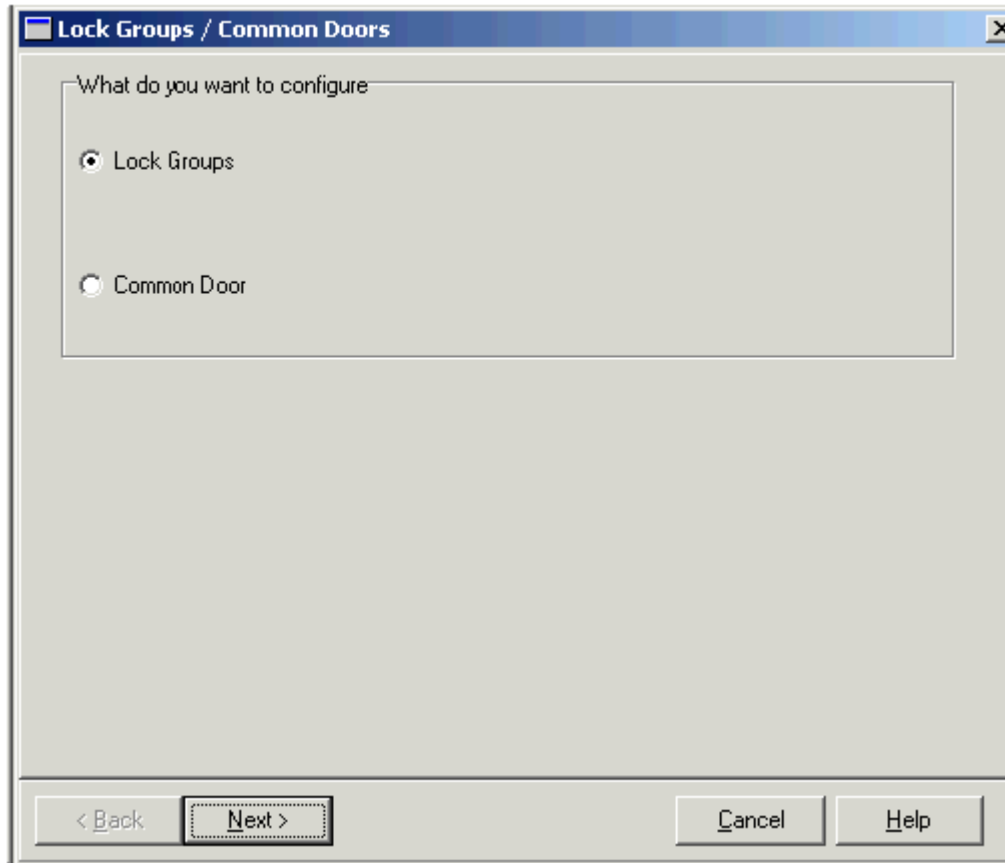
Option	Description
EV/ES Number	This number is assigned by VingCard. It is entered when Vision is installed. It is used as the product license number.
Facility Code	Each hotel has its own unique Facility Code. It is used to identify the property. Keycards issued from one Facility Code are not valid in any other Facility Code.

New code entry

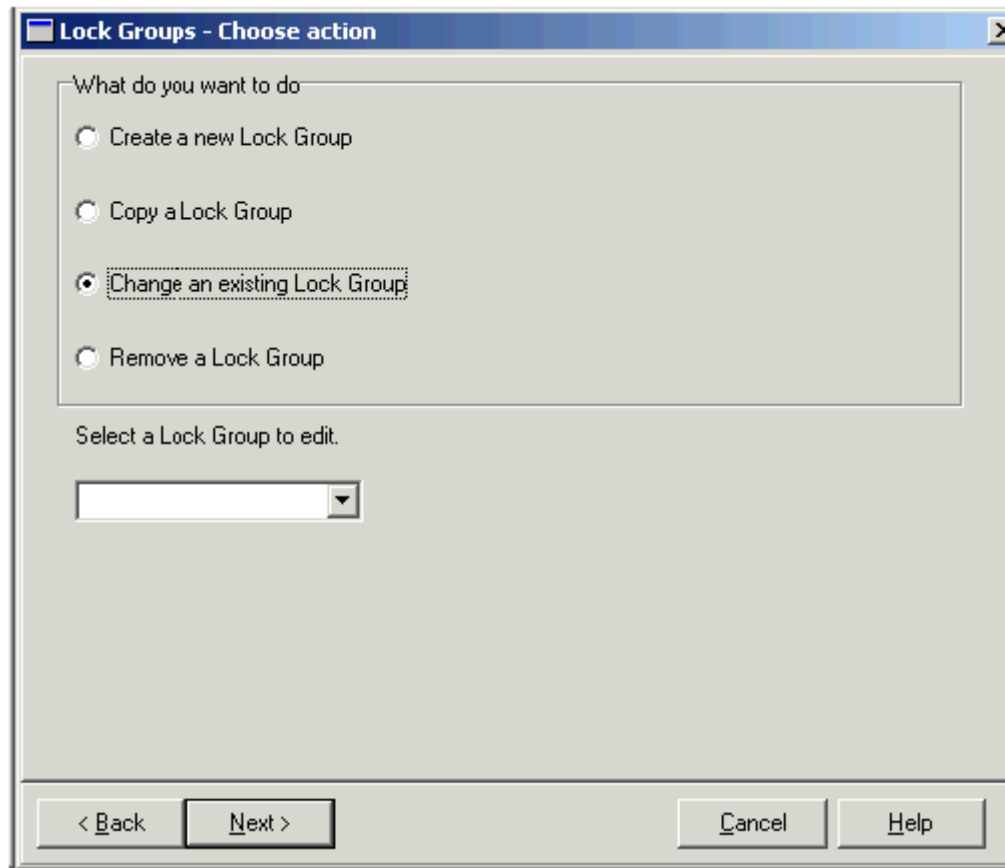
Enter new license agreement number here to increase the limits at your Hotel

Locks Wizard

Locks - Lock Groups or Common Door



Option	Description
Lock Groups	Use the Lock Group button of the Lock Wizard to create custom, guest door, and lift controller Lock Groups. The wizard will take you through all of the necessary steps, including the Lock Mode selection and the creation of Time Tables.
Common Door	When you have finished, click the Common Doors button to designate Common Doors. You will be able to select from all of the locks in the Lock Groups you created. The ability to copy any existing User Groups, Common Door settings, and Time Tables speeds the amount of time required to set up Lock Groups.

Locks - Create, Copy, Change, Remove

Option	Description
Create New Lock Group	Creates a new Lock Group.
Copy a Lock Group	Allows you to easily create a new Lock Group with new names but similar settings.
Change an Existing Lock Group	Allows you to modify an existing Lock Group.
Remove a Lock Group	Deletes a Lock Group.

Locks - Name of Lock Group

Lock Groups - Change - PAX CABINS

Lock Group name:

PAX CABINS

Lock Group

☒ Guest door locks

☐ Lift Controllers / MDCs

☐ Custom locks

< Back Next > Cancel Help

Option	Description
Name of Lock Group	Type a unique name for the Lock Group.
Lock Group Selection	Select whether the lock(s) you are creating are for Guest Door Locks , Lift Controllers (elevators), or Custom (special settings). TIP: Select custom if you want locks in the lockgroup to stay unlocked under various conditions – either at fixed times of day or when activated with a special ‘Stay Unlocked’ enabled guest keycard.

Locks - Motor Selection

Lock Groups - Changing - PAX CABINS

Lock motor

☒ Vingcard

☐ Custom

☐ Duration

☐ Pulse width (msec): 50

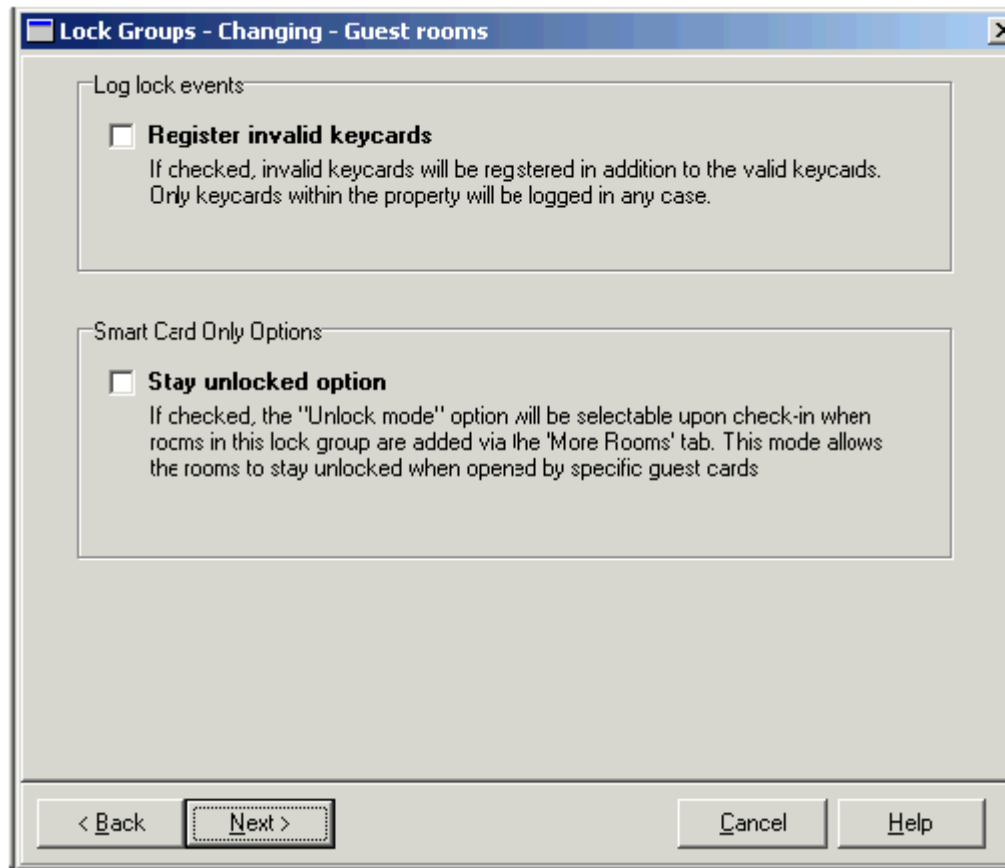
Unlock time

Unlock time (1-255 sec): 6

< Back Next > Cancel Help

Option	Description
VingCard	Motor manufactured by VingCard.
Custom (Motor)	<p>Special Lock - you will need to specify the Duration and Pulse Width required by the lock.</p> <p>Most often, these are devices connected to a remote reader. However, you may also want to select this for VingCard motors that require a long or shorter pulse.</p>
Unlock Time	How long the lock will remain unlocked to allow someone to pass through.

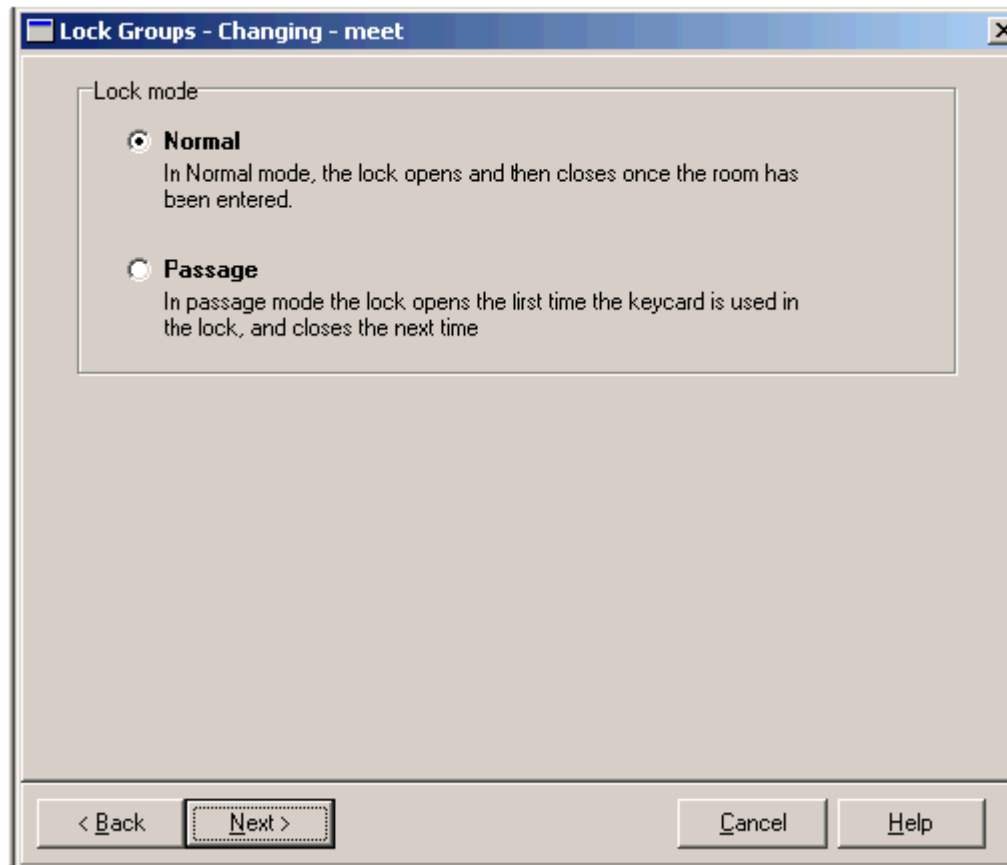
Locks – Special Options



Option	Description
Register Invalid Keycards	<p>All valid keycards that access the locks will always generate an entry in the lock's event log. Attempts by non-valid keycards to open a lock in this lockgroup will only be logged if this option is checked.</p> <p>For security purposes, keycards with a different Facility Code are not recognized between different hotels. Therefore, they will never be logged.</p> <p>TIP: you may not want to use the storage space within the lock by logging information about those who did not actually open the door.</p> <p>NOTE : this setting DOES NOT affect the 'Entry Log' information that can be stored on individual Smart Cards. The entry log will always show the doors the Smart Card has opened and NEVER the doors it has attempted to open but failed.</p>
Stay Unlocked Option	<p>This will only work for Da Vinci, Presidio and VC3000 Combo locks.</p> <p>Unlock mode allows selected guest keycards special access to doors such as conference rooms. Thus, a conference leader can be issued with a keycard that gives normal access to their own room, but also 'Stay Unlocked' access to a conference room.</p>

	<p>This means the conference leader's key will open the conference room door when inserted, and the door will remain unlocked (for the other delegates) until the conference leader uses their key again – at which time the door locks.</p> <p>To make this work, the 'special' rooms (for example Conference Rooms) should be grouped in a single lock group. This lock group should be of type 'Custom Locks' (first page in wizard) and the 'Stay Unlocked' option should be checked. You do NOT need to select Passage mode on the next Wizard page.</p> <p>To make the 'Conference Leader' style keycards, the selected Conference Room(s) are selected as Additional Rooms during Guest Check In. An option then appears, which if checked will cause the keycard to work in 'Stay Unlocked' mode. If not checked, the keycard will simply access the Conference Room in the normal way (i.e. door will unlock and automatically relock when the key is used).</p> <p>NOTE : remember to add the locks in the 'stay unlocked' lock group into the accessible rooms under keycard setup for the necessary guest keycard types – that is, the keycard types that will be issued to the 'Conference Leader' type guests.</p>
--	---

Locks - Normal or Passage Mode



Option	Description
Normal (Mode)	Locks in the lockgroup will only remain unlocked during the time specified on the "Unlock Time" you specified earlier in

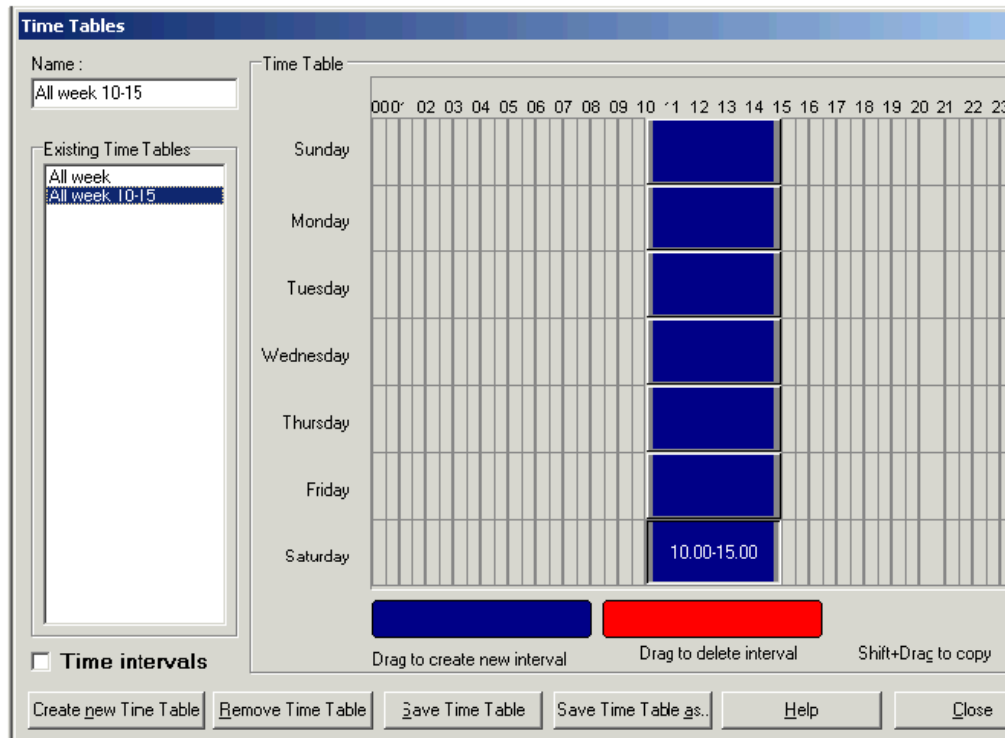
	the Wizard (a few seconds). After that, it automatically relocks.
Passage (Mode)	<p>After being unlocked, locks in the lockgroup will remain unlocked until a keycard is inserted again. In other words, it toggles between locked and unlocked as keycards when valid keycards are used in it.</p> <p>NOTE unlike 'Stay Unlocked' mode (previous wizard page) this will apply to ALL keycards used in the locks.</p>

Locks - Lock Open Time Table

If you selected **Custom** for the Lock Group, this Time Table screen will appear to allow you to control whether a lock remains unlocked based on the time of day.

Option	Description
Off/On	Select Off if you do not want the lock to remain unlocked at certain times of the day
Time Table	If you selected On , you can either select an existing Time Table, or click the Edit Time Table button to change or create a Time Table.

Locks - Edit Time Table



Option	Description
Existing Time Tables	To delete or change, or copy a Time Table, select from this list, then click on one of the buttons across the bottom of the window. If you want to create a new Time Table, just select the Create New Time Table button.
Time Intervals checkbox	Click on this to turn on/off the display of the time for each line of the Time Table. (This has no affect on the functionality of the Time Table, it is just displayed for your convenience.)
Deleting Interval	Click on the blue button, and then drag to where you want the interval to start. When you release the mouse, a cell will be coloured. Drag on the double arrows to shade the time for the Time Table interval.
Adding an Interval	Click on the red button, and then drag to the interval you want to remove. When you release the mouse, it will be erased.
Copying an Interval	Hold shift and click on an interval. Drag it to where want to copy to and release the mouse.

Locks - Building and Adding Lock Names

This screen is where lock names are created. There are two methods for accomplishing this depending on whether you want to create locks individually or multiple locks at one time:

Method 1 - Creating multiple locks at a time:

Lock Groups - Create new - Block Seven

Locks to install in group

Prefix: B7 Range: 01 to 10 Build

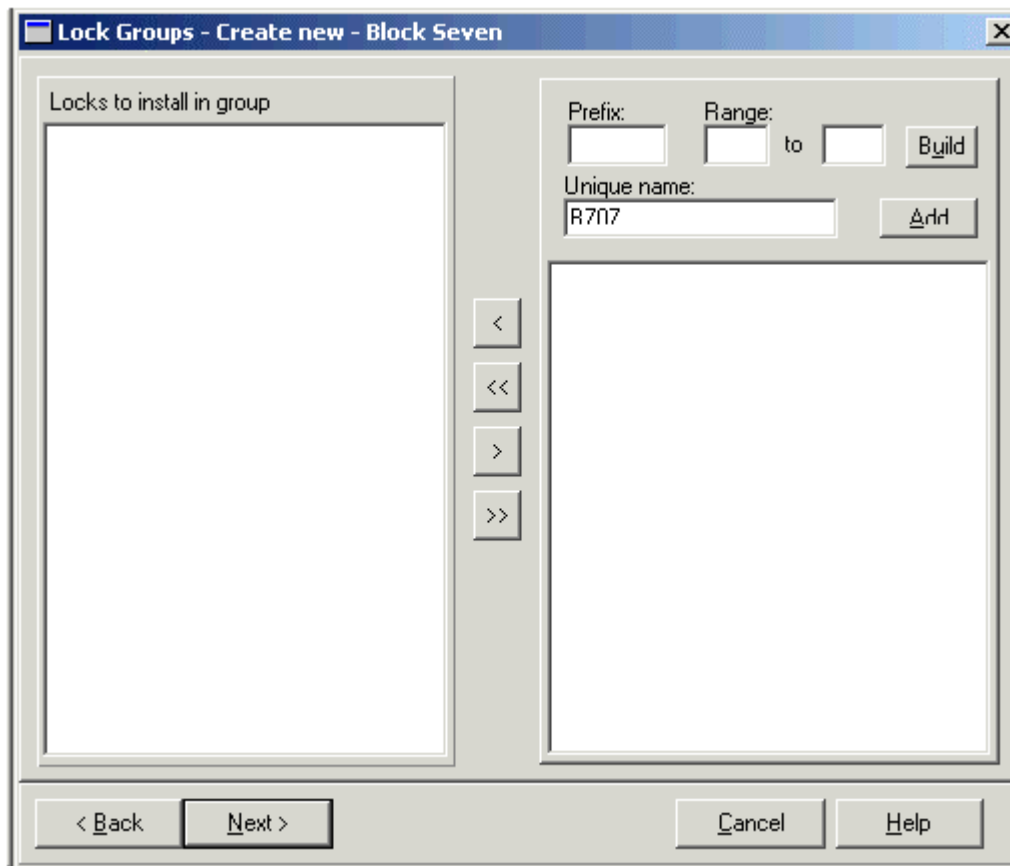
Unique name: Add

< << > >>

< Back Next > Cancel Help

Option	Description
Prefix	Optionally type character(s) for the new lock names to begin with. If you leave this blank, just the Range will be used.
Range (from)	Type a starting number for the new lock names.
Range (to)	An ending number for the new lock names. For example if the range is 100 to 500, locks would be created beginning with names from 100 through 500. TIP: If not all of the lock names are needed, (for example if there is no room 425) you can still create the entire range and will be able to omit it as explained later in this Help topic.
Build	When you finish entering the Prefix and Range, click the Build button to list the locks in the right-hand window of the screen. Repeat the above process if necessary to list all of the locks you want available for this Lock Group.
Selecting Locks from the list	You are NOT required to select all of the locks in the window: <i>To select several locks in a row - Hold the Shift key and click on the first and last item you want to select (all items between will be shaded.)</i> <i>To select locks individually - Hold the Ctrl key and click on</i>

	<p><i>each of the lock names that you want to select (each lock name will be shaded.)</i></p> <p><i>TIP:</i> <i>If you want to select all locks, it is not necessary to shade any of them.</i></p>
Arrow buttons	<p>To move locks between the two windows:</p> <p><i>When you have finished shading locks for selection, use the single arrow button to move them to the other window.</i></p> <p><i>OR</i></p> <p><i>To move all locks to the other window, click the double arrow button.</i></p> <p>You can move items between the two windows with the arrow buttons at any time. The double arrows will move all items and the single arrows will move only shaded items.</p>

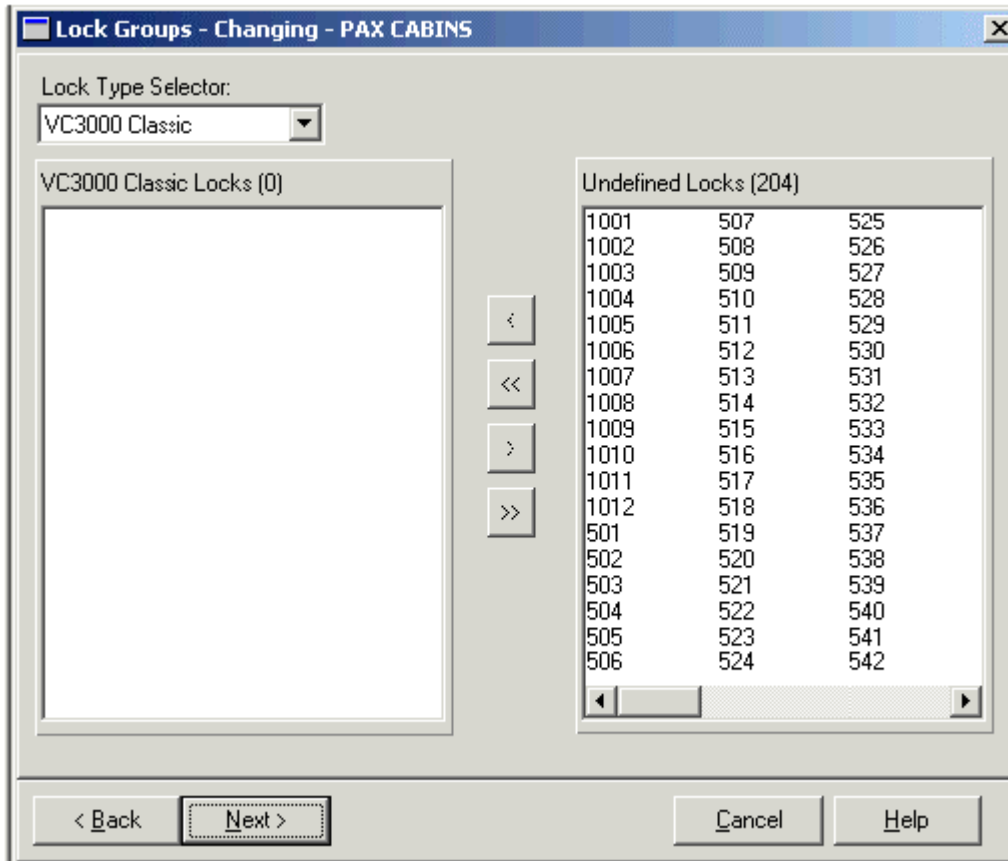
Method 2 - Creating one lock at a time:

Option	Description
Unique Name	Type the name of the new lock.
Add button	<p>Click the Add button to list the locks in the right hand window of the screen.</p> <p>Repeat the above process if necessary to list all of the locks you want available for this Lock Group.</p>
Arrow buttons	You can move items between the two windows with the arrow buttons at any time. The double arrows will move all items and the single arrows will move only shaded items.

Locks – Assigning a Lock Types to each Lock

After specifying all locks in the lock group (previous wizard page) you must now assign a specific Lock Type to each lock. Examples of Lock type are VC3000 Classic, Presidio or Da Vinci. This information allows Vision to determine which lock program and data to load to each lock, and what types of keycard it can accept – for example mag-stripe cards or Smart Cards.

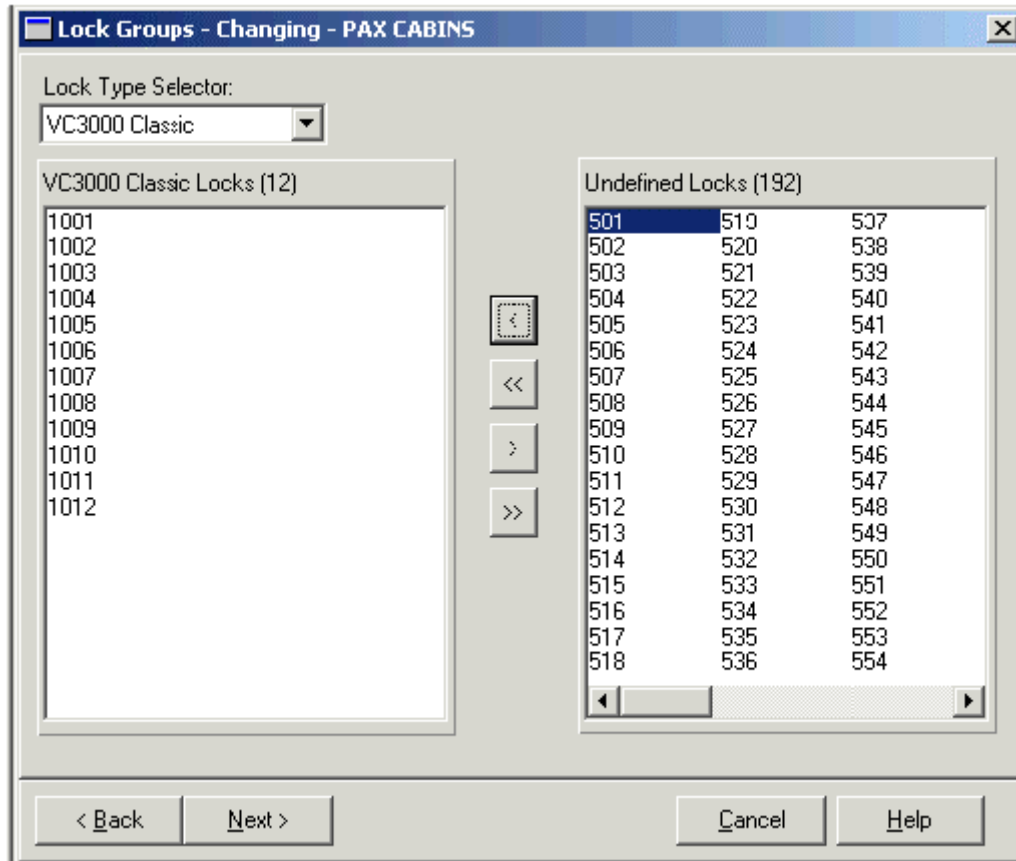
Initially, all locks will be Unassigned – that is, not associated with any lock type.



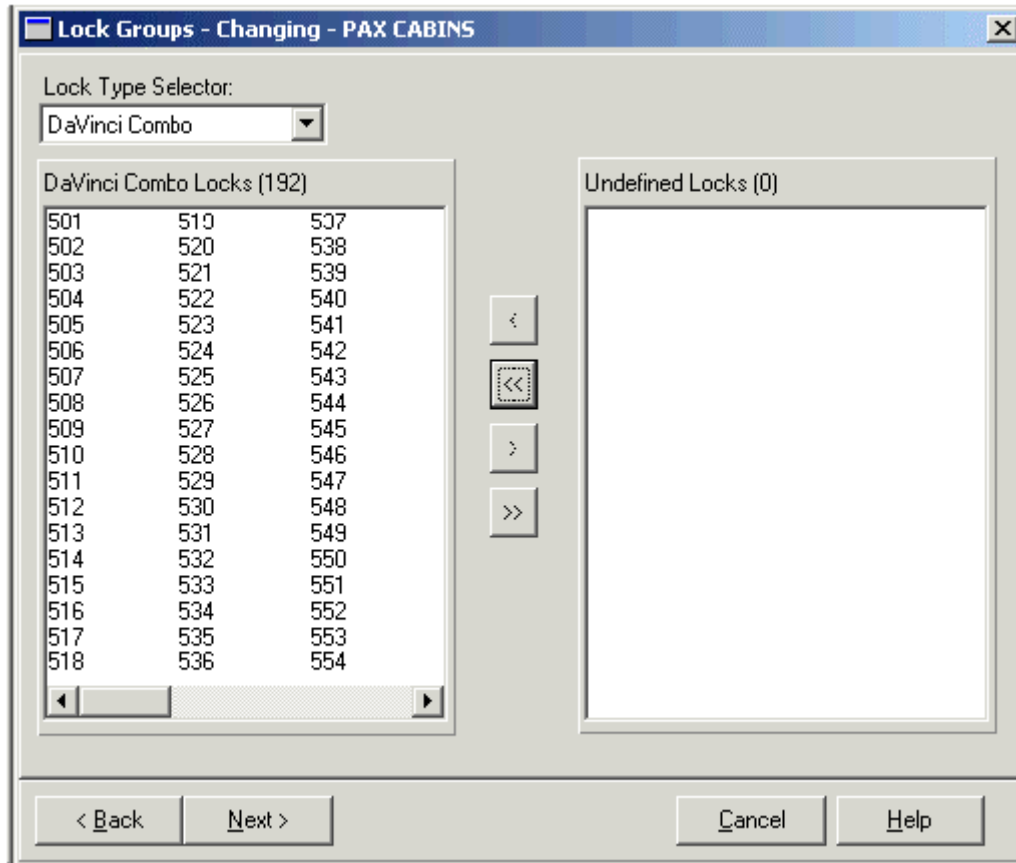
Option	Description
Lock Type Selector	Select a Lock Type to assign some (or all) of the locks to
Arrow buttons	You can move items between the two windows with the arrow buttons at any time. The double arrows will move all items and the single arrows will move only selected items.

Example :

Say some of the locks in the lockgroup are of type VC3000 Classic, some of type Da Vinci Combo. First, select VC3000 Classic in the Lock Type Selector. Then highlight the locks of this type from the 'Unassigned' list and use the arrow keys to move them across to the VC3000 list on the left.



Now select the next lock type (Da Vinci Combo), and move the remaining locks over to the left hand list.



Assign all locks until the 'Unassigned' count is 0. Then press **Next**.

NOTE : Do not leave locks unassigned. This will leave Vision unable to determine fully the lock characteristics. LockLink WILL NOT program unassigned locks.

Locks - Results of Wizard

Lock Groups - Changing - PAX CABINS

Lock Group name:	PAX CABINS	Lock open Time Table:	Off
Lock Group:	Guest door locks	Logging:	Log only valid keycards
Lock motor:	Vingcard	Unlock mode option:	Not selectable
Lock mode:	Normal	Licenced number of locks :	2000
Unlock time:	6 sec	Total number of locks in system :	396
		Number of locks in this group :	204

View Time Table

Lock Type Selector: DaVinci Combo Lock count = 192

501	508	515
502	509	516
503	510	517
504	511	518
505	512	519
506	513	520
507	514	521

< Back Next > Finish Cancel Help

Displays information about the Lock Group you just created or edited. If there is anything you want to change, you can click the **Back** button and make changes.

Locks Common - Door Type

Common Doors

Common Door type

☒ **Standard lock / Remote Controller**
Standard lock / Remote Controller is typically used for sauna, main entrance, parking lot etc.

☐ **Lift Controller / MOC**
Lift Controller / MOC has 7 relay contacts for use in elevators, parking areas etc.

< Back Next > Cancel Help

Select either **Standard Lock/Remote Controller** or **Lift Controller/MOC**.

Common Doors – How many can be configured?

You can always configure up to 53 Common Doors – but it is important to realise that depending on the type of keycards you make, you might not be able to pass information about all 53 to a keycard :

If you **do not** use the 'More Rooms' feature when checking in guests:

- Information about all 53 common doors can be written to a mag-stripe card
- the first 7 bits are reserved for the MOC (Lift Controller) leaving 46 other useable definable common doors
- if your property uses old style VingCard Safes (NOT Elsafe) then the 'Safe Option' which can be enabled on guest cards will use Common Door position 53. Therefore, you should define a maximum of 45 common doors to avoid conflict.

If you **do** use the 'More Rooms' feature when checking in guests:

- adding 1 'More Room' to a mag-stripe card will restrict you to 49 common doors per card. Number 49 is reserved in case the Safe Option is required, so only 1 to 48 can actually be selected and written to the card. Of these, the first 7 bits are reserved for the MOC (Lift Controller).
- adding 2 'More Rooms' to a mag-stripe card will restrict you to 14 common doors per card. Number 14 is reserved in case the Safe Option is required, so only 1 to 13 can actually be selected and written to the card. Of these, the first 7 bits are reserved for the MOC (Lift Controller).

If you use Smart Cards

- there are no restrictions, so you can always pass all 53 common doors to each card. The Safe Option is not an issue with Smart Cards – because VingCard Safes only read mag-strip cards. Therefore Common Door 53 is always available.

Locks Common - Create, Change, Remove

Unless you selected Lift Controller/MOC, the following screen will be displayed.

Common Doors - Choose an action

Common Door

☒ Make a new Common Door

☐ Change an existing Common Door

☐ Remove an existing Common Door

Common Door not available.

< Back Next > Cancel Help

Option	Description
Make a New Common Door	Designates a lock as a Common Door.
Edit an Existing Common Door	Change an existing Common Door selection.
Remove an Existing Common Door	Removes designation of Common Door from locks with this Common Door Name.

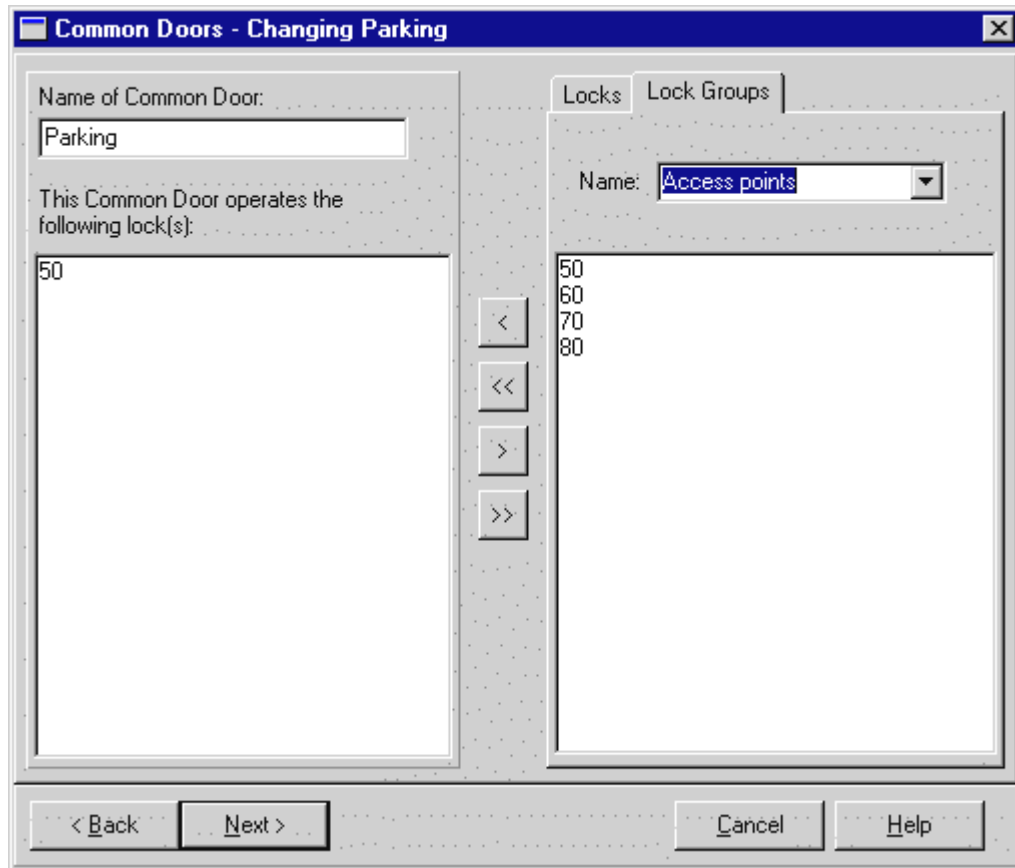
Locks Common - Name of Common Door and Selection of Locks

This screen is where Common Door names are created and locks are assigned to them. There are two methods for accomplishing this depending on whether you want to assign Common Doors to individual locks or to Lock Groups.

Method 1 - Individual Locks (Locks tab):

Option	Description
All	List all locks.
Odd	List only Odd numbered locks
Even	List only Even numbered locks
Step	Skips the display of some locks based on the number you enter. For example, if you specify 3, only every third lock in the list will be displayed.

Update List button	After making selections, click this button to refresh the list.
Selecting Locks from the list	<p>You are NOT required to select all of the locks in the window:</p> <p><i>To select several locks in a row</i> - Hold the Shift key and click on the first and last item you want to select (all items between will be shaded.)</p> <p><i>To select locks individually</i> - Hold the Ctrl key and click on each of the lock names that you want to select (each lock name will be shaded.)</p> <p><i>TIP:</i> If you want to select all locks, it is not necessary to shade any of them.</p>
Arrow buttons	<p>To move locks between the two windows:</p> <p><i>When you have finished shading locks for selection, use the single arrow button to move them to the other window.</i></p> <p><i>OR</i></p> <p><i>To move all locks to the other window, click the double arrow button.</i></p> <p>You can move items between the two windows with the arrow buttons at any time. The double arrows will move all items and the single arrows will move only shaded items.</p>

Method 2 - Lock Groups (Lock Groups tab):

Option	Description
Name	The list to select from will either display Lock Groups that you created as Lift Controller/MOCs or Custom locks depending on which you selected earlier in this wizard.
Arrow buttons	You can move items between the two windows with the arrow buttons at any time. The double arrows will move all items and the single arrows will move only shaded items.

Locks Common - Lift Relay Contacts

If you selected Lift Controller/MOC as the Common Door type, the following screen will be displayed.

Common Doors - Setting up relay contacts

Choose the relay contact to configure

Lift Controller/MOC

☐ lift 4th floor Relay contact 1

☒ lift 5th floor Relay contact 2

☐ <none> Relay contact 3

☐ <none> Relay contact 4

☐ <none> Relay contact 5

☐ <none> Relay contact 6

☐ <none> Relay contact 7

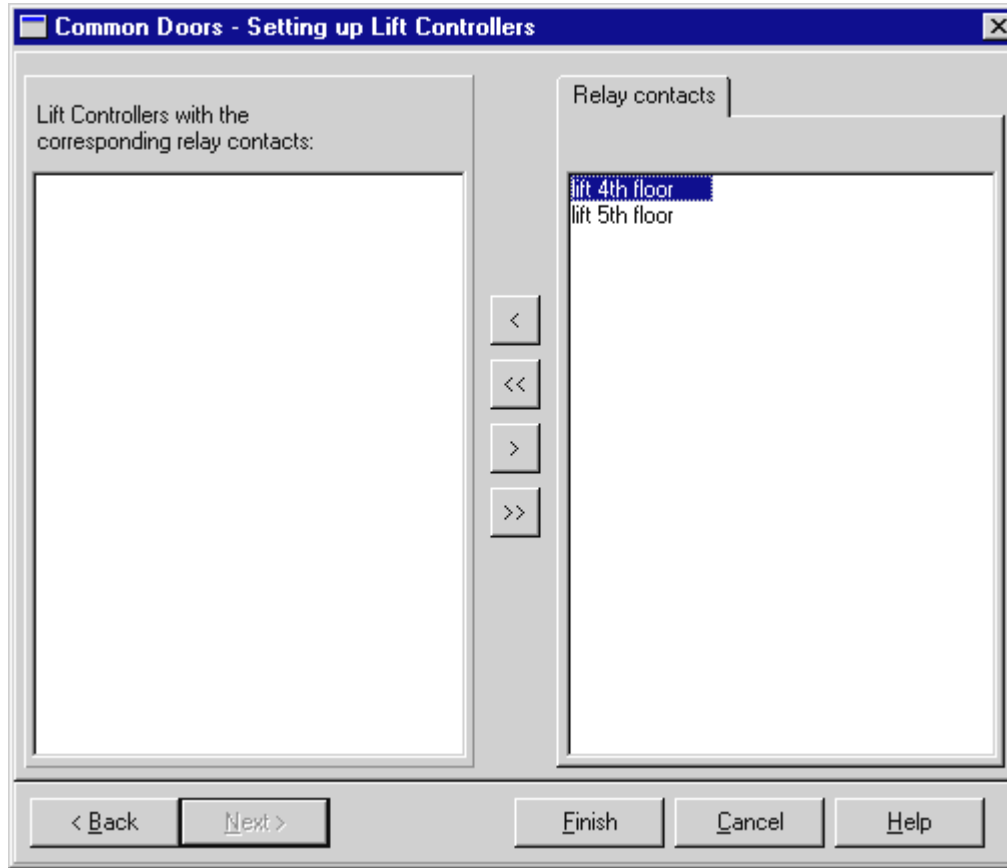
Name of relay contact:

lift 5th floor Add Delete selected

< Back Next > Cancel Help

This screen is used to name the Relay Contacts so that you do not have to remember them as Relay contact 1 and so on.

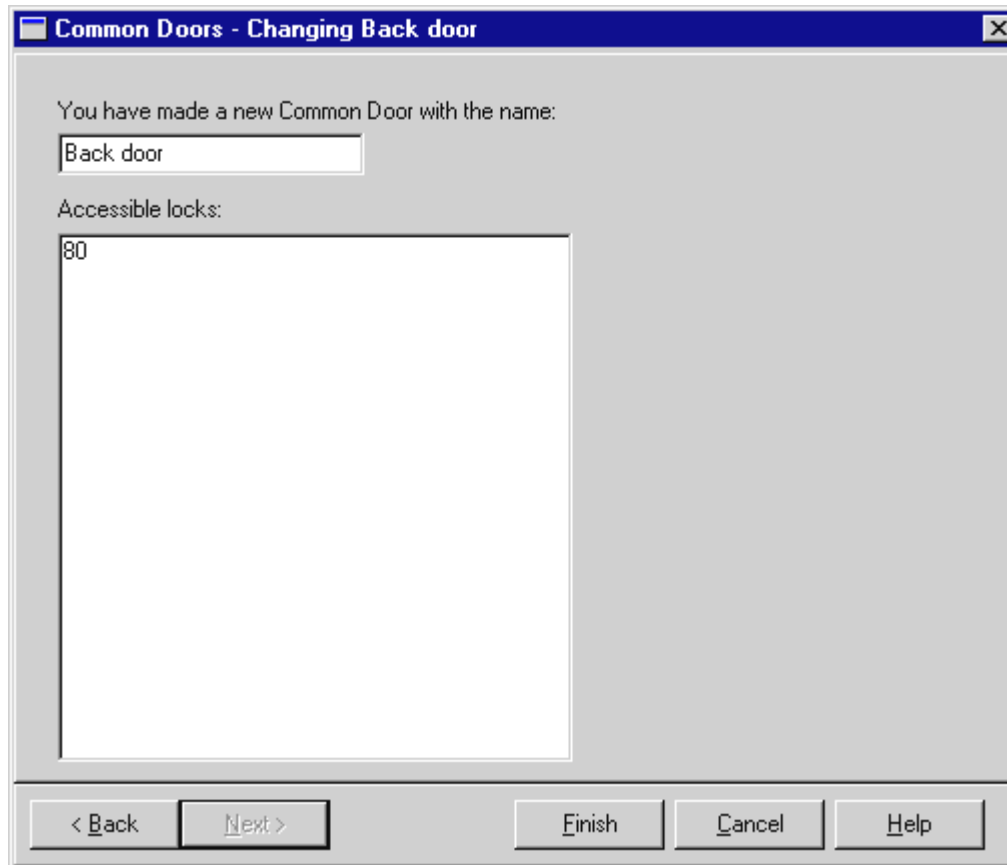
Option	Description
<none> selections	These are displayed as <none> until you rename them. Click on the radio button of the relay contact you want to rename.
Name of Relay Contact	Type the name you want to assign to this relay contact.
Add button	Click to assign the new name to the relay contact. You can continue to name all of the relay contacts at this time if you wish.
Delete Selected button	Return the name to <none>.

Locks Common - Lift Controllers

Option	Description
Lift Controllers with the corresponding relay contacts	Select a lift controller.
Relay Contacts	Select which relay contacts will be included with the lift controller.

Locks Common - Results of Common Wizard

Displays information about the Common Doors you just created or edited. If there is anything you want to change, you can click the **Back** button and make changes.



Keycard Types Wizard

Keycard Type - Create Keycard Type

Keycard type

What do you want to do

☒ Create new Keycard Type

☐ Create new Keycard Type based on existing

☐ Change existing Keycard Type

☐ Remove a Keycard Type

Keycard Type not available

Edit Sections

< Back Next > Cancel Help

Option	Description
Create new Keycard Type	Creates a new Keycard Type.
Create new Keycard Type based on existing	Allows you to easily create a new Keycard Type similar to an existing one.
Change existing Keycard Type	Allows you to modify an existing Keycard Type.
Remove a Keycard Type	Deletes a Keycard Type.
Edit Sections button	<p>Starts the Edit Sections Wizard which is used to create and change sections. (You can think of this as a wizard within a wizard.)</p> <p>TIP: You will also be able to access the Edit Sections Wizard later in the Keycard Types Wizard. Whenever you finish with it, you will be returned to where you left off in the Keycard Type Wizard.</p>

Keycard Type - Select Keycard Type

Keycard Type - Change - Employee room

Name of Keycard Type:

Keycard Type

Guest

- ☐ **Rooms**
This type is the single guest room. Typically all guest rooms will be of this type.
- ☐ **Suites / Connected rooms**
This will create the suite rooms for guests.

Employee

- ☒ **Rooms**
This is single employee rooms.
- ☐ **Sections**
This is employee sections, typically used when setting up access for maids, housekeeping etc.

< Back Next > Cancel Help

All Keycard Types are either Guest (normally either guests or one-shot) or Employee (maid, staff, security, etc.)

Option	Description
Name of Keycard Type	The name of the Keycard Type you are changing or creating.
Guest	<p>Rooms—Select this if you want to set up guest Keycard Types for individual rooms.</p> <p>Suite—Select this only if you want to set up Keycard Types for suites or combined rooms.</p>
Employee	<p>Rooms—Select this if you want to set up employee Keycard Types for individual rooms.</p> <p>Suite—Select this only if you want to set up employee Keycard Types for suites or combined rooms.</p>

Keycard Type - Override Criterion

Keycard Type - Change - Employee room

Override Criterion

☒ **Issue Time**
A Keycard with a valid time window will override and cancel if it is issued at a later time and has a later or equal Start Time.

☐ **Start Time**
A Keycard will only override if its Start Time is later than the former Keycard.

< Back Next > Cancel Help

Keycards can be overridden (made invalid) by another keycard. The most common usage of this is to invalidate the previous guest's keycard when a newer keycard is used in the lock.

Use this screen to specify whether you want this Keycard Type to be overridden based on the creation date/time or the time that the keycard is set to open locks.

Option	Description
Issue Time	Select this if you want the time that the keycard was encoded to be the criteria for overriding. Normally, hotels will select this option.
Start Time	Select this if you want the time that the keycard becomes valid in the lock to be the criteria for overriding. Normally, only cruise ships or other situations where there is a delay between the time a keycard is issued and the time it becomes valid will select this option.

TIP: For one-shot Keycard Types, it does not matter which you select as they invalidate themselves.

Keycard Type - Select Type of Suite

If you selected Guest Suite for type of keycard, the following screen will display:

Keycard Type - Change - Suite

Select which type of suites to create

☐ Two rooms

☒ Three rooms

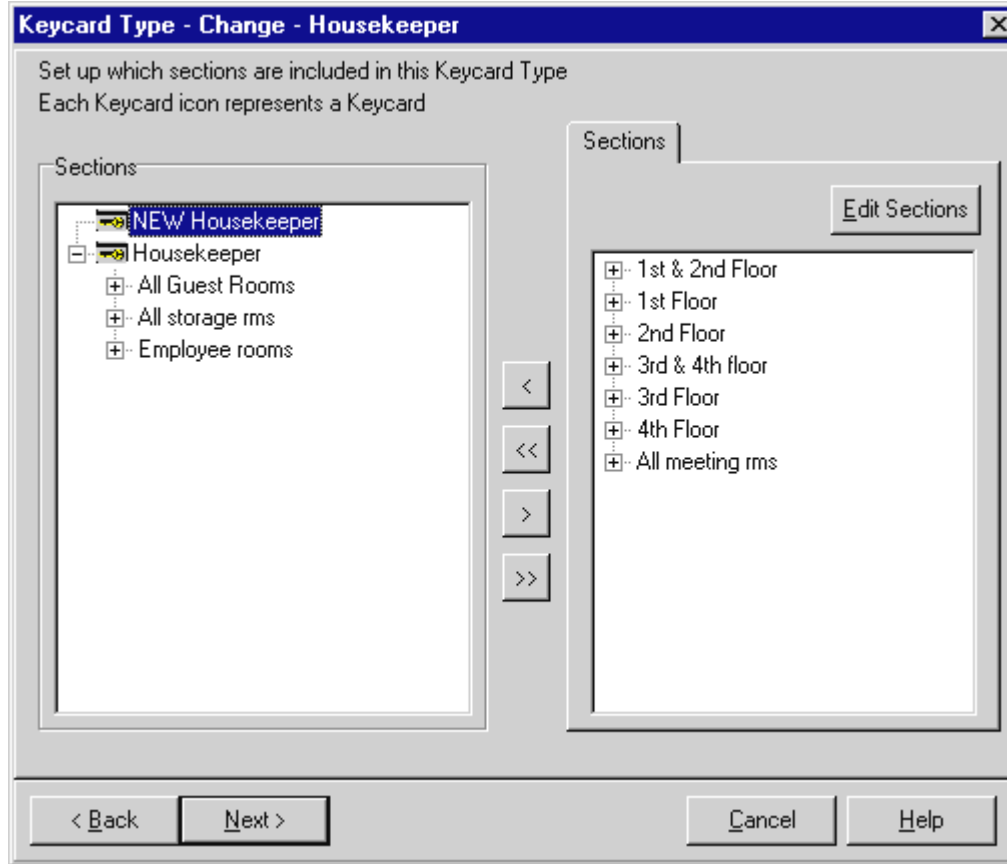
☐ Rooms

< Back Next > Cancel Help

Option	Description
Two Rooms	Select the number of rooms in this suite. If more than three, you can type the number of rooms.
Three Rooms	
or specify number	

Keycard Type - Select Employee Sections

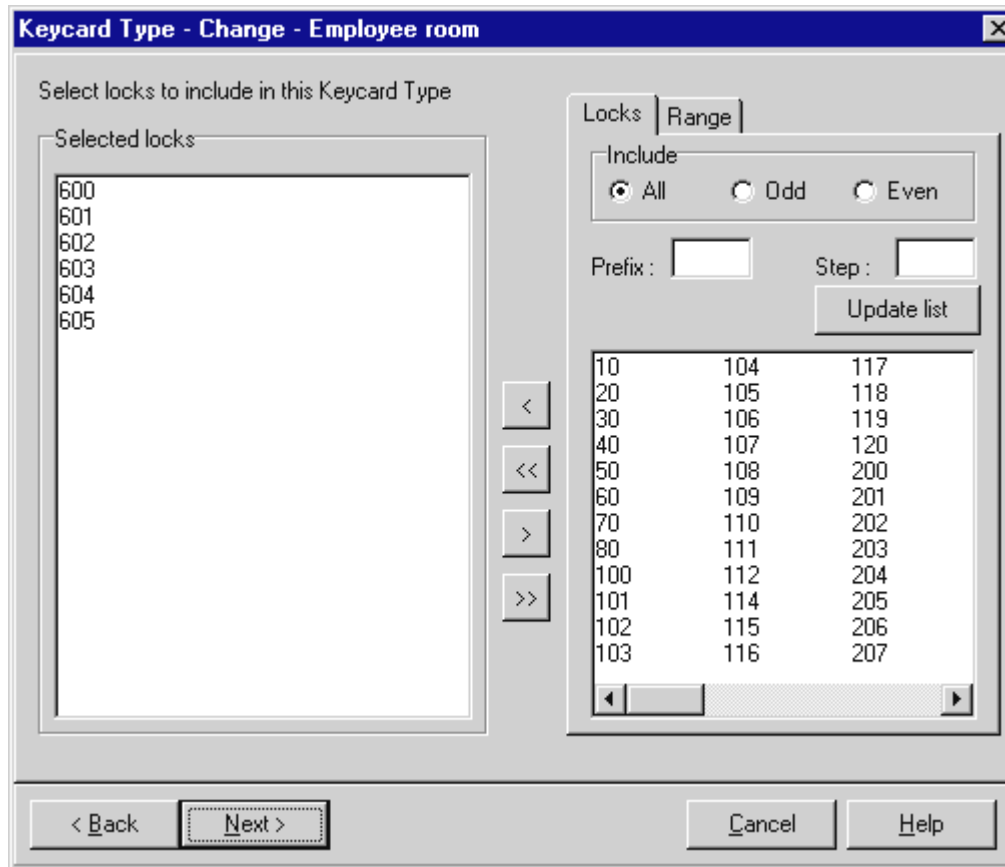
This screen appears when you are creating or editing Keycard Types for Employee Sections.



Option	Description
Adding Keycard Types and assigning sections to them.	<p>The name you specified will be displayed on this screen with "New" appended to the beginning of it.</p> <p>Click on it and then select a section (from the window on the right.) Notice that another keycard type icon is added to the window (using the and the section is assigned to it.</p> <p>To assign more sections to the keycard, click on it in the left window and select more sections from the right window.</p> <p>To create new keycards to assign sections to, click on the "New" keycard (top of the list) and repeat the process.</p> <p>TIP: Later when you create User Groups, you will be able to select from these Keycard Types that are associated with sections.</p>
Edit Sections button	<p>Select this if you want to create, remove, or change sections to assign them to Keycard Types. It will take you to the Edit Sections Wizard. When you have finished using it, you will be returned to this screen.</p>

Keycard Type - Select Employee or Guest Rooms

There are two methods of displaying the list of employee room or guest room locks depending on whether you want to select from all locks or a range of locks:



Method 1 - Selecting from a list of all locks (Locks tab):

Option	Description
All	List all locks.
Odd	List only Odd numbered locks
Even	List only Even numbered locks
Step	Skips the display of some locks based on the number you enter. For example, if you specify 3, only every third lock in the list will be displayed.
Update List button	After making selections, click this button to refresh the list.
Selecting Locks from the list	<p>You are NOT required to select all of the locks in the window:</p> <p>To select several locks in a row - Hold the Shift key and click on the first and last item you want to select (all items between will be shaded.)</p> <p>To select locks individually - Hold the Ctrl key and click on each of the lock names that you want to select (each lock name will be shaded.)</p> <p>TIP: If you want to select all locks, it is not necessary to shade</p>

	<i>any of them.</i>
Arrow buttons	<p>To move locks between the two windows: <i>When you have finished shading locks for selection, use the single arrow button to move them to the other window.</i></p> <p><i>OR</i></p> <p><i>To move all locks to the other window, click the double arrow button.</i></p> <p>You can move items between the two windows with the arrow buttons at any time. The double arrows will move all items and the single arrows will move only shaded items.</p>

Method 2 - Selecting from a Range of locks (Range tab)

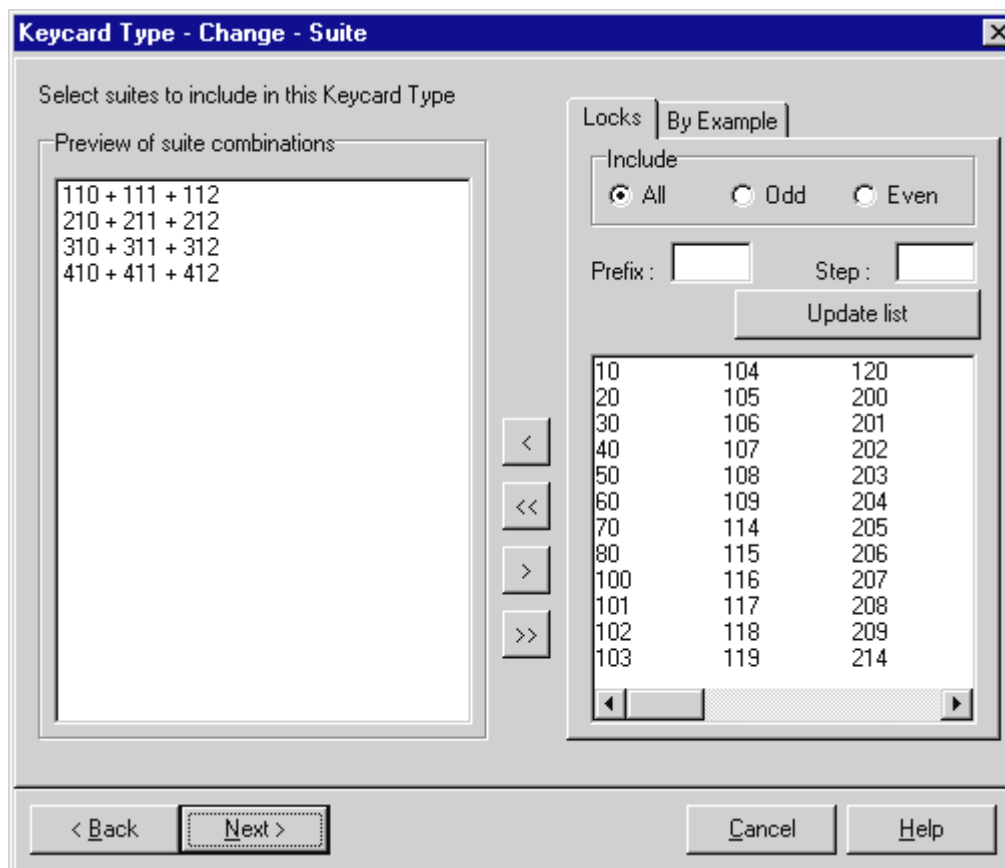
The screenshot shows a window titled "Keycard Type - Change - Employee room". Inside, there's a section "Select locks to include in this Keycard Type". On the left, under "Selected locks", is a list box containing the numbers 600, 601, 602, 603, 604, and 605. On the right, there's a "Range" tab with "From" and "To" input fields, both containing the number 600 and 605 respectively. Below these fields is a "Build range" button. Between the list box and the range fields are four arrow buttons: a single left arrow, a double left arrow, a single right arrow, and a double right arrow. At the bottom of the dialog are four buttons: "< Back", "Next >", "Cancel", and "Help".

<p>Range tab</p> <p>Displays the list of locks based on a range of lock numbers.</p>	<p>From - type a starting number To - type an ending number</p> <p>Build range button - after making entries, click this button to refresh the list.</p>
---	--

Keycard Type - Select Guest Suites

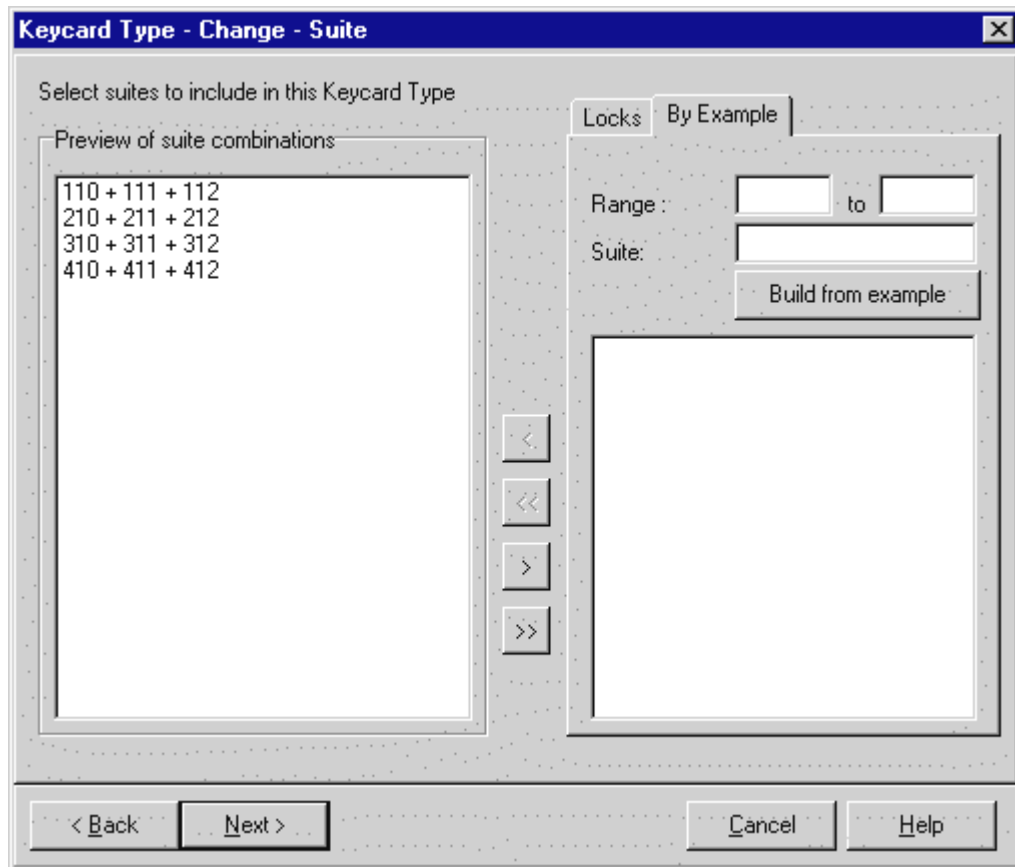
Use one of these two methods of selecting suites for this Guest Keycard Type.

Method 1 - Selecting from a list of All, Odd, Even, by Prefix. or by Step:



Option	Description
Locks Tab	Lists all room numbers.
All	
Odd	Lists all odd numbered locks.
Even	Lists all even numbered locks.
Prefix	Type in one or more characters to display all locks beginning with this number.
Step	Type in a number to increment by. For example, if you typed 3, each third match to your criteria would be displayed. If left blank, all matches will be displayed.
	Click the Update List button to refresh the list after making selections.

Method 2 - Selecting from a list based on an example:



By example tab	<p>From - type a starting number</p> <p>To - type an ending number</p> <p>Suite - type the name of a suite</p> <p>Click the Build from Example button to refresh the list after making selections.</p>
-----------------------	---

Keycard Type - Select Interrelation

Keycard Type - Change - Suite

Set up how this Keycard Type interrelates with other Keycard Types

Cancels | Cancelled by | ☐ Interrelates to itself (One Shot)

Will cancel

- <Fail safe>
- Single Room
- Connecting 0/1
- Connecting 1/2
- Connecting 0/2

Will not cancel

- Banquet dept
- Employee room
- Housekeeper
- Maid
- Maid 2 Floors
- Maintenance
- Master
- Mini bar
- One shot
- Room Service
- Security

Cancels - Select which Keycard Types this
Cancelled by - Select which Keycard Types will cancel this Keycard Type

< Back Next > Cancel Help

Use the arrow keys to move one or all items between the two windows.

Option	Description
Cancels tab	Which Keycard Types this Keycard Type will override. For example, you would normally want all of the guest Keycard Types to override all of the other guest Keycard Types. This would prevent the previous guest from accessing the room. You would also probably want to override the fail-safe Keycard Type.
Cancelled by tab	Which Keycard Types (if any) will override this Keycard Type. Quite often, the Cancels list will be the same as the Cancelled by list. However, this is not a requirement.
Interrelates to itself (one-shot) check box	If you check this, the keycard will override itself. In other words, it will never be valid after being used once. You might want to do this to allow someone, such as a repair person, to enter a room only one time.

Keycard Type - Finish

Keycard Type - Change - Suite

You have now created a Keycard Type with the following parameters

Name : Suite

Type : Guest Section

Override Criterion
☒ Issue Time ☐ Start Time

☐ Interrelates to itself (One Shot)

Cancels Cancelled by

<Fail safe>
Single Room
Connecting 0/1
Connecting 1/2
Connecting 0/2

Rooms :
110 + 111 + 112
210 + 211 + 212
310 + 311 + 312
410 + 411 + 412

< Back Next > Finish Cancel Help

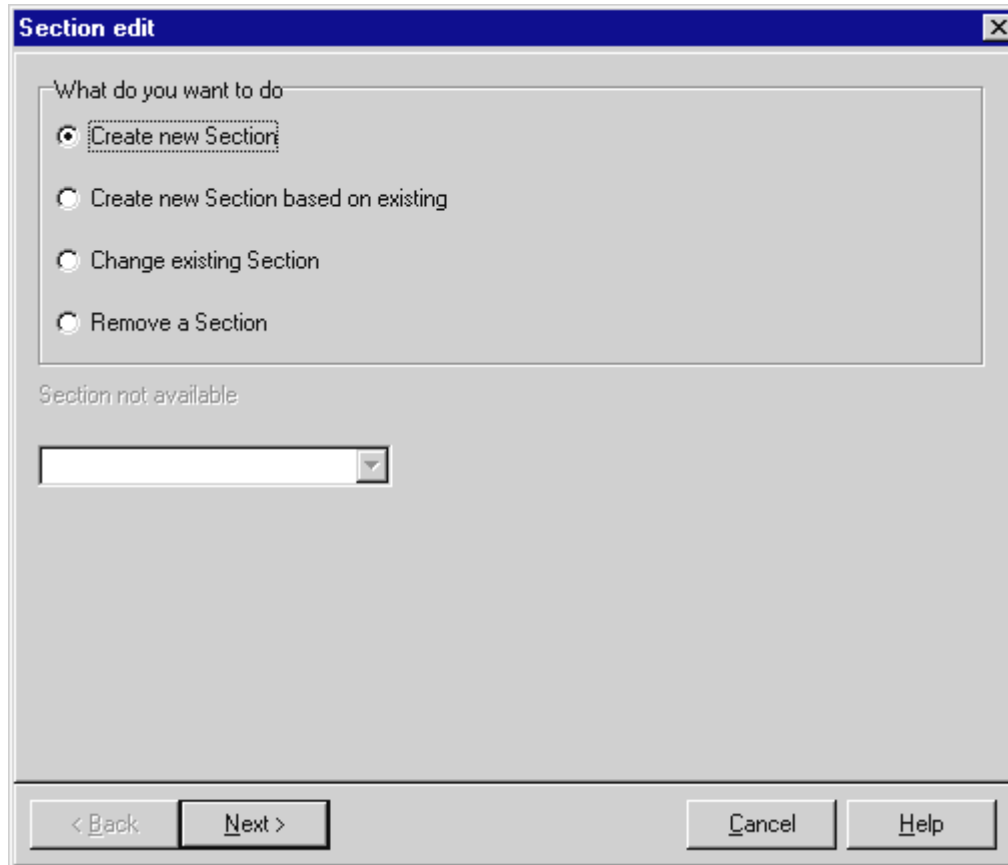
Displays information about the Keycard Type you just created or edited. If there is anything you want to change, you can click the **Back** button and make changes.

Keycard Type - Edit Sections Menu

This Edit Sections Wizard assists you in creating or changing a section. It is actually a wizard within a wizard.

It is launched when you select the Edit Sections button from the first screen of the Keycard Types Wizard. It can also be launched from the fourth screen of the Keycard Types Wizard.

When you finish with this wizard, you will be returned to where you left off in the Keycard Type Wizard.



Option	Description
Create New Section	Creates a new Section.
Copy a Section	Allows you to easily create a new Section with new names but similar settings.
Change an Existing Section	Allows you to modify an existing Section.
Remove a Section	Deletes a Section.

Keycard Type - Edit Sections Window

Select one of the following three methods of displaying the list of locks and then use the arrow keys to move one or all items between the two windows.

Method 1 - Selecting from a list of All, Odd, Even, by Prefix, or by Step:

Section - Change - All Guest Rooms

Section: All Guest Rooms

Locks in Section

100	119	217
101	120	218
102	200	219
103	201	220
104	202	300
105	203	301
106	204	302
107	205	303
108	206	304
109	207	305
110	208	306
111	209	307
112	210	308
114	211	309
115	212	310
116	214	311
117	215	312
118	216	314

Locks | Lock Groups | Range

Include: ☒ All ☐ Odd ☐ Even

Prefix: Step:

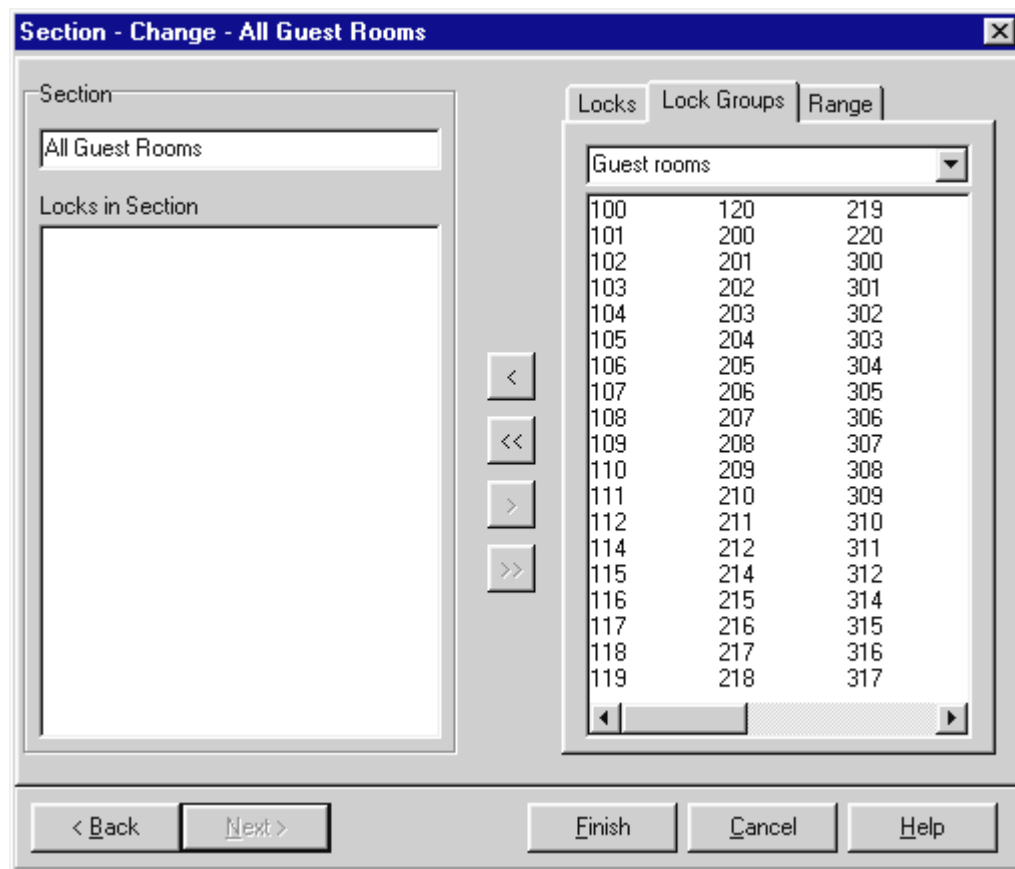
Update list

10 600
20 601
30 602
40 603
50 604
60 605
70
80
500
501
502
503
504
505

< << > >>

< Back Next > Finish Cancel Help

Option	Description
All	Lists all room numbers.
Odd	Lists all odd numbered locks.
Even	Lists all even numbered locks.
Prefix	Type in one or more characters to display all locks beginning with this number.
Step	Type in a number to increment by. For example, if you typed 3, each third match to your criteria would be displayed. If left blank, all matches will be displayed.

Method 2 - Selecting from a list of all locks in a Lock Group:

Lock groups tab
Displays the list of
locks based on your
Lock Groups.

Click on the drop down list and select a Lock Group.

Method 3 - Selecting from a Range of lock names:

The screenshot shows a software window titled "Section - Change - All Guest Rooms". It has three tabs: "Locks", "Lock Groups", and "Range". The "Range" tab is active. On the left, there is a "Section" label and a text box containing "All Guest Rooms". Below this is a "Locks in Section" label and a large empty list box. To the right of the list box are four navigation buttons: "<", "<<", ">", and ">>". Further right are the "From" and "To" input fields, both containing the number 100 and 300 respectively. Below these fields is a "Build range" button. At the bottom of the window are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

100	117	212
101	118	214
102	119	215
103	120	216
104	200	217
105	201	218
106	202	219
107	203	220
108	204	300
109	205	
110	206	
111	207	
112	208	
114	209	
115	210	
116	211	

Range tab

Displays the list of locks based on a range of lock numbers.

From - type a starting number

To - type an ending number

Build range button - after making entries, click this button to refresh the list.

User Groups Wizard

User Groups - Create, Copy, Change, Remove

User Groups

What do you want to do

- ☒ Create a new User Group
- ☐ Create a new User Group based on previous
- ☐ Change existing User Group
- ☐ Remove a User Group

User Group not available

< Back Next > Cancel Help

Option	Description
Create New User Group	Creates a new User Group.
Create a New User Group Based on Previous	Allows you to easily create a new User Group similar to an existing one.
Change an Existing User Group	Allows you to modify an existing User Group.
Remove a User Group	Deletes a User Group.

User Groups - Name of User Group

User Groups - Create new -

Name of User Group: All Guest Rooms

User group

☒ Guest Rooms / Sections

☐ Employee Rooms

☐ Employee Section

< Back Next > Cancel Help

Option	Description
Name of User Group	The name of the User Group you are changing or creating.
Guest Rooms/Sections	Select this if the User Group is for Guests.
Employee Rooms	Select this if the User Group is for Employees and the access is for individual rooms or locks.
Employee Sections	Select this if the User Group is for Employees who will need access to the sections (created with the Keycard Types Wizard.) Normally this will be for maids, housekeeping, and so on.

User Groups - Deadbolt Override and Safe Default

User Groups - Change - V.I.P Guest

Default settings

☒ **Deadbolt override**
This is a default setting that allows a card issued for this group to open doors with deadbolt in use.

☐ **Safe access**
This is a default setting that allows a card issued for this group to use the safe.

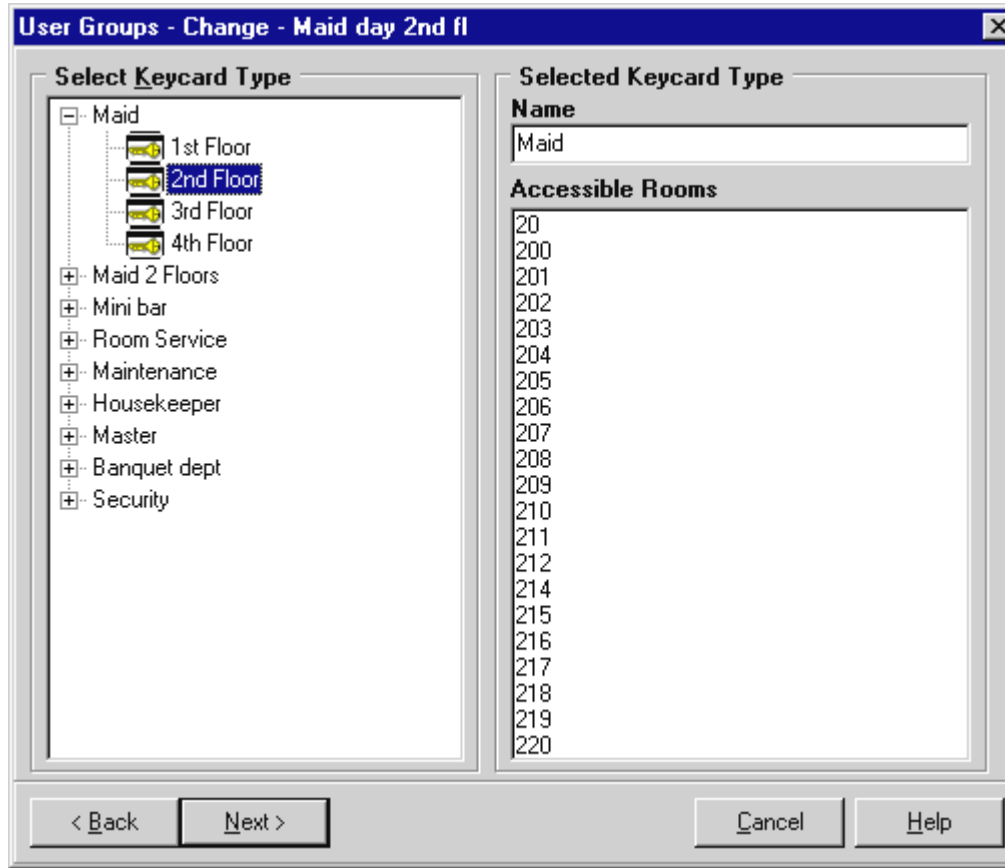
Smart card only settings

☐ **Reset after cylinder tamper alarm**
This is a default setting that allows a card issued for this group to reset the lock, which was blocked by a metal key.

☒ **Entry Log**
This is a default setting that allows a card issued for this group to carry an entry log, detailing which rooms have been entered.

< Back Next > Cancel Help

Option	Description
Deadbolt Override	Select this only if you want the keycard holders to be able to open doors when the deadbolt is thrown from the inside.
Safe Access	Select this if you offer keycard access to safes and you want some or all of this User Group to be able to access them. If you check this box, you will be able to assign this capability to individuals in this User Group when issuing keycards.
Reset After cylinder tamper alarm	Only relevant for User groups that carry Smart Cards. Only relevant for locks equipped with metal-key cylinders. Allows cards issued for this user group to reset locks that are out of use due to a cylinder tamper alarm. The light on the lock will be flashing red for this alarm. It indicates a forced entry was attempted.
Entry Log	Only relevant for User groups that carry Smart Cards. Enables an entry log to be stored on the Smart Cards of card holders in the user group. An entry log allows a report to be made showing which rooms the card has been used to enter.

User Groups - Keycard Type for Employee

Option	Description
Select Keycard Type window	Double click to expand and contract the list. Select the Keycard Type you want to create a User Group for. The accessible rooms will be displayed in the right window.

User Groups - Start and End of Employee Keycards

User Groups - Change - Maid day 2nd fl [X]

Duration

Start: 4 / 2 / 98 8 : 04 : 00 PM

End: 4 / 1 / 00 8 : 04 : 00 PM

of days: 730

This parameter specifies how long a card issued for this User Group will be valid. If new User Groups are created based on the same Keycard Type, all User Groups will inherit the same duration.

Other user groups sharing the same keycard type

Name	Start time	End time

< Back Next > Cancel Help

Option	Description
Start/End Date	<p>Using the Calendar to change the start and end (expiration) date:</p> <p><i>To display the previous or next month, click the arrow at the top left or right of the calendar.</i></p> <p><i>To display a list of months to select from, click on the name of the month.</i></p> <p><i>To select a day, click on the day of the month in the calendar.</i></p>
Start/End Time	Set the time of day the keycard will become valid and the time of day it will expire.
# of days	How many days this keycard will remain valid.
Other Groups Sharing this same Keycard Type	The User Groups that will be affected by the selections on this screen.

User Groups - Select Time Table

User Groups - Change - Employee room [X]

You have to select a Time Table for cards belonging to the User Group.

All week [v]

Preview of Time Table:

	am												pm												
	12	01	02	03	04	05	06	07	08	09	10	11	12	01	02	03	04	05	06	07	08	09	10	11	12
Monday	12.00am-12.00am																								
Tuesday	12.00am-12.00am																								
Wednesday	12.00am-12.00am																								
Thursday	12.00am-12.00am																								
Friday	12.00am-12.00am																								
Saturday	12.00am-12.00am																								
Sunday	12.00am-12.00am																								

Edit Time Tables

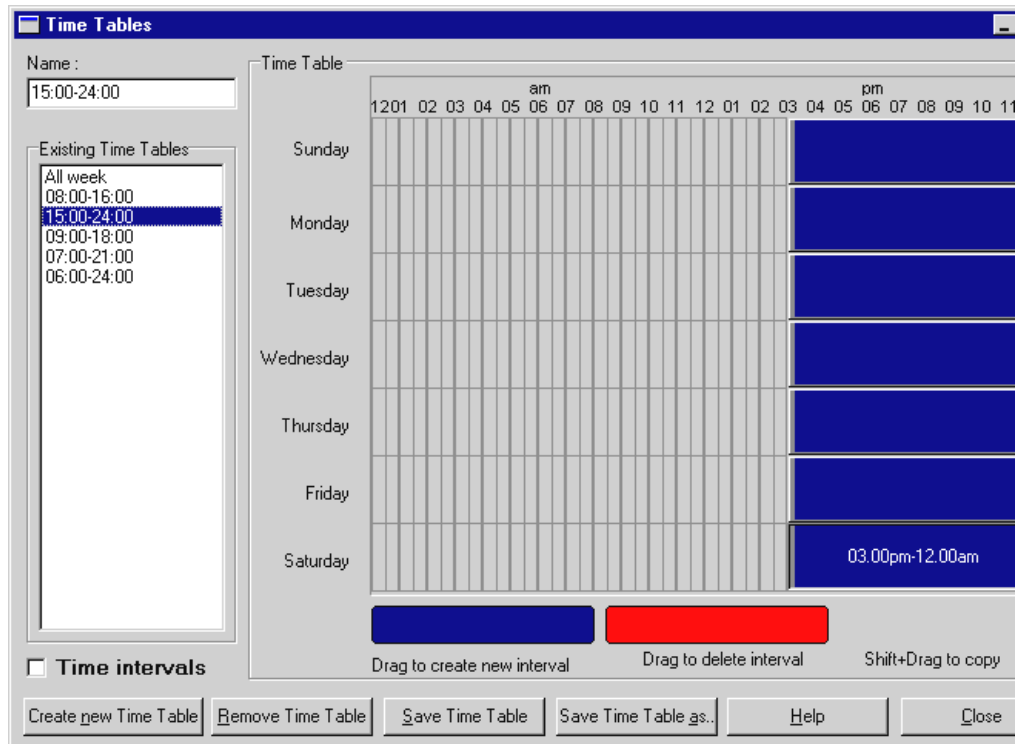
< Back Next > Cancel Help

The Time Tables you created in the Keycard Types Wizard will be available. You can optionally create new Time Tables in the User Group Wizard.

Option	Description
Time Table	<p>Select a Time Table for this User Group. Normally guests will be assigned a Time Table that allows access at all times.</p> <p>You should create a User Group for each group of employees that need a different Time Table. For example, you might want one group of maids to have keycard access from 9:00 am to midnight and another group to have access from midnight to 9:00 am.</p>

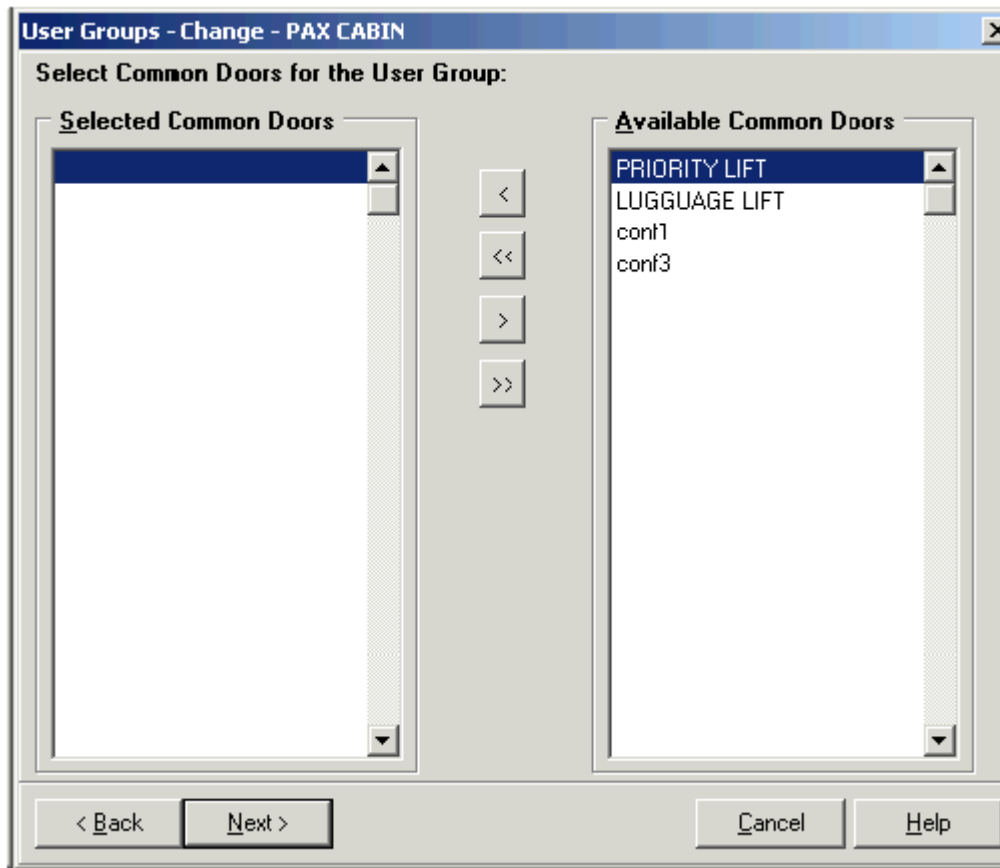
Click the Edit Time Table button to create, delete or edit a Time Table.

User Groups - Edit Time Table



NOTE: Keycard Types and User Groups share the same Time Tables.

Option	Description
Existing Time Tables	<p>To delete or change, or copy a Time Table, select from this list, then click on one of the buttons across the bottom of the window.</p> <p>If you want to create a new Time Table, just select the Create New Time Table button.</p>
Time Intervals checkbox	<p>Click on this to turn on/off the display of the time for each Interval (line of the Time Table.)</p> <p>TIP: This has no affect on the functionality of the Time Table, it is only displayed for your convenience.</p>
Deleting Interval	<p>Click on the blue button, and then drag to where you want the interval to start.</p> <p>When you release the mouse, a cell will be coloured. Drag on the double arrows to shade the time for the Time Table interval.</p>
Adding an Interval	<p>Click on the red button, and then drag to the interval you want to remove. When you release the mouse, it will be erased.</p>
Copying an Interval	<p>Hold shift and click on an interval. Drag it to where want to copy to and release the mouse.</p>

User Groups - Common Doors

To select Common Doors individually - Hold the Ctrl key and click on each of the lock names that you want to select (each lock name will be shaded.)

Use the arrow buttons to move items between the Selected and Available windows.

Option	Description
Selected Common Doors	These Common Doors will be available for selection when issuing keycards for anyone in this User Group.
Available Common Doors	All of the locks for guests, or employees (depending on whether you selected Guest or Employee on a previous screen of this wizard) will be displayed.

User Groups - Time Tables for Common Doors

User Groups - Change - Maid night 3/4

You have to select a Time Table for every Common Door:

Common Door	Time Table
lift 4th floor	15:00-24:00
Back door	15:00-24:00

All week
08:00-16:00
15:00-24:00
09:00-18:00
07:00-21:00
06:00-24:00

Time Table for currently selected Common Door:

	am												pm												
	12	01	02	03	04	05	06	07	08	09	10	11	12	01	02	03	04	05	06	07	08	09	10	11	12
Monday																									
Tuesday																									
Wednesday																									
Thursday																									
Friday																									
Saturday																									
Sunday																									

03.00pm-12.00am

< Back Next > Cancel Help

This screen appears if you selected Common Doors to include with this User Group.

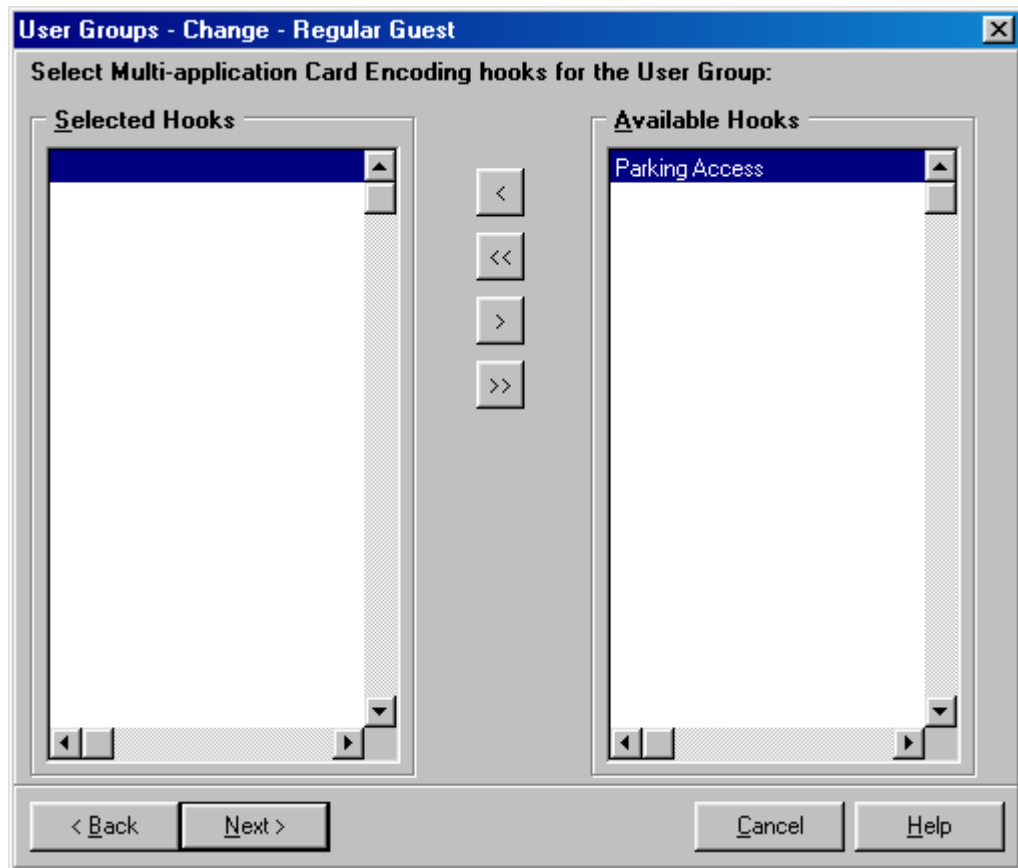
Option	Description
Common Door	All of the Common Doors that you selected earlier in this wizard will be listed.
Time Table	When you click on the Time Table cell, an arrow will be displayed. Click on it to select a Time Table for this Common Door. Repeat for each Common Door.
Default	Any Common Doors that are set to "On" will automatically be selected when keycards are issued. You can override this setting when issuing keycards by deselecting Common Doors.

User Groups – MACE (Multi-application Card Encoding)

You can assign Multi-application Card Encoding (MACE) 'hooks' to each user group in a similar way to assigning common doors.

A MACE is an external software module (a DLL) written by third party developers. If selected and assigned to a 'Guest Rooms / sections' type user group, then whenever a card for the user group is made, the external DLL will be called such that customised data can be written to mag-stripe tracks 1 and / or 2.

Full details on MACE module, including a developers guide is included in a separate MACE manual.



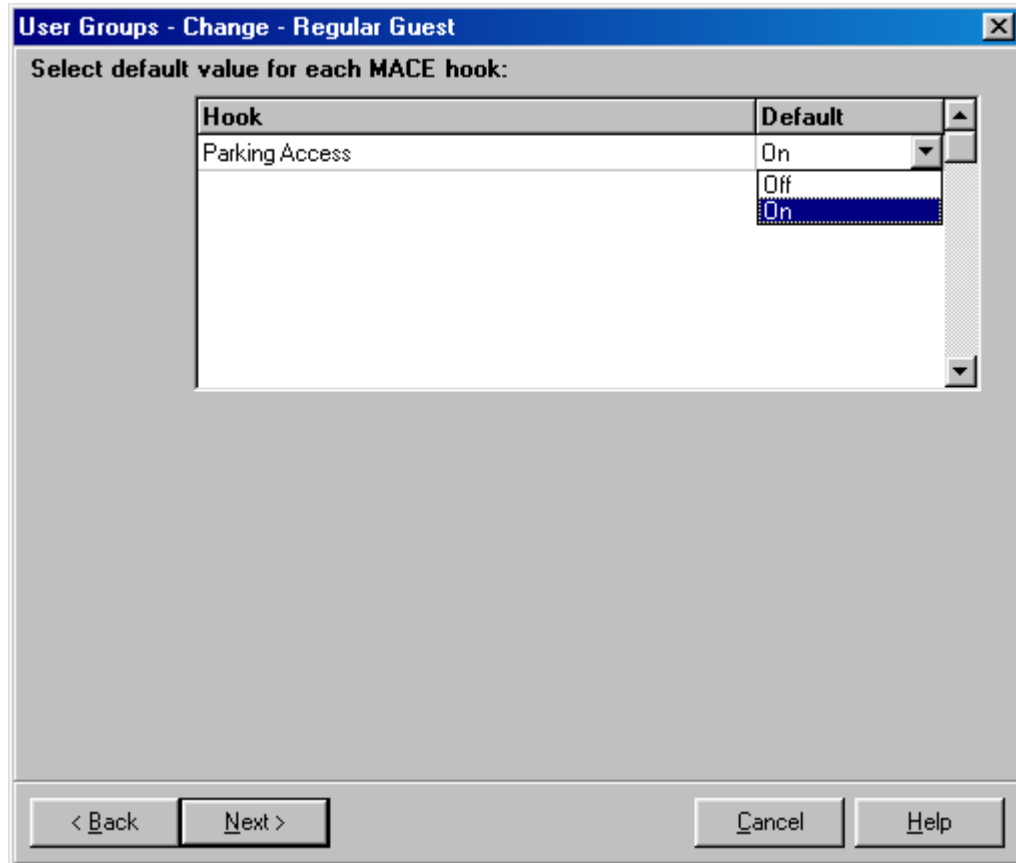
To select MACE hooks individually - Hold the Ctrl key and click on each of the hook names that you want to select (each name will be shaded.)

Use the arrow buttons to move items between the Selected and Available windows.

Option	Description
Selected Hooks	These hooks will be available for selection when issuing keycards for anyone in this User Group.
Available Hooks	All of the possible hooks for guests will be displayed. Note

	that these have to be defined and activated in Setup > System parameters > MACE tab
--	--

User Groups – Defaults for each MACE hook



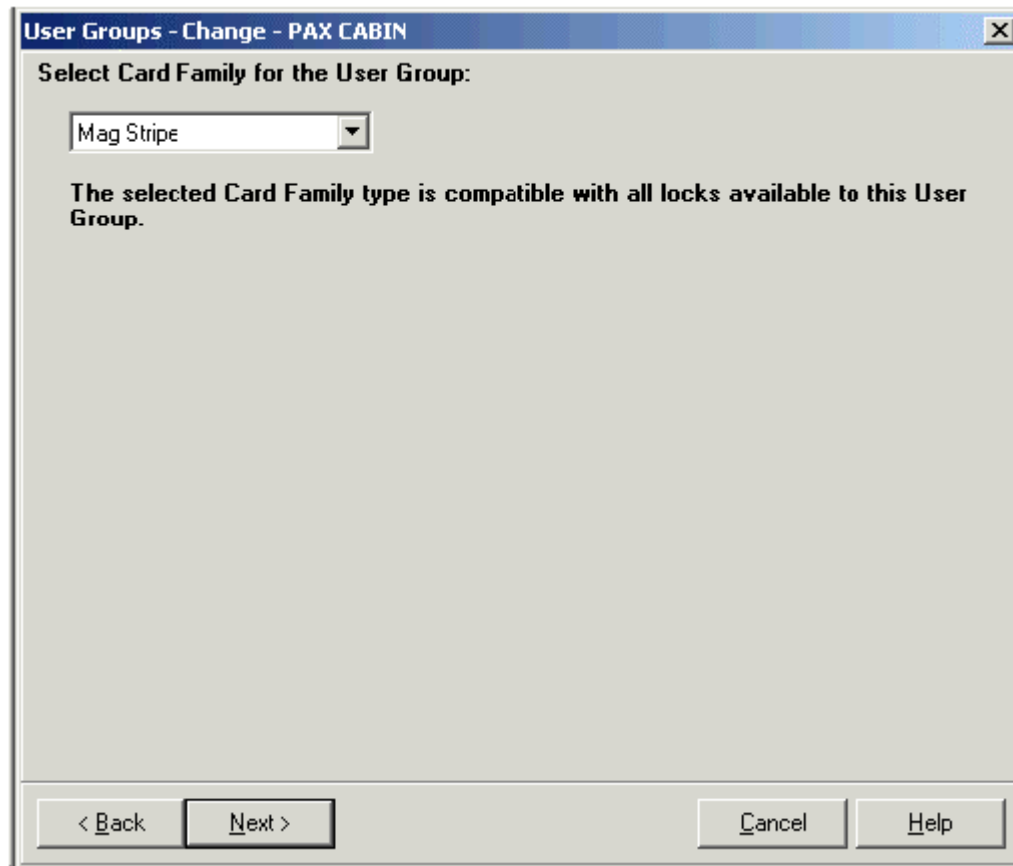
Option	Description
Hook	Each hook made available to the user group on the previous page is listed
Default	On or Off. This determines whether the MACE hook is called by default whenever keycards are made for this user group – i.e. if you do not make further adjustments before making a keycard. The actual setting can be changed on a card-by-card basis prior to encoding the card – just like Common Door defaults. Thus if a hook defaults to ‘on’ you can still make a card that does not call the hook, and vice versa.

User Groups – Select Card Family

You must assign a ‘Card Family’ (for example **mag-stripe** or **Smart Card**) to each user group. This determines which type of keycards will be encoded for members of the user group member.

Assigning card family type by user group avoids prompting for type each time a card is

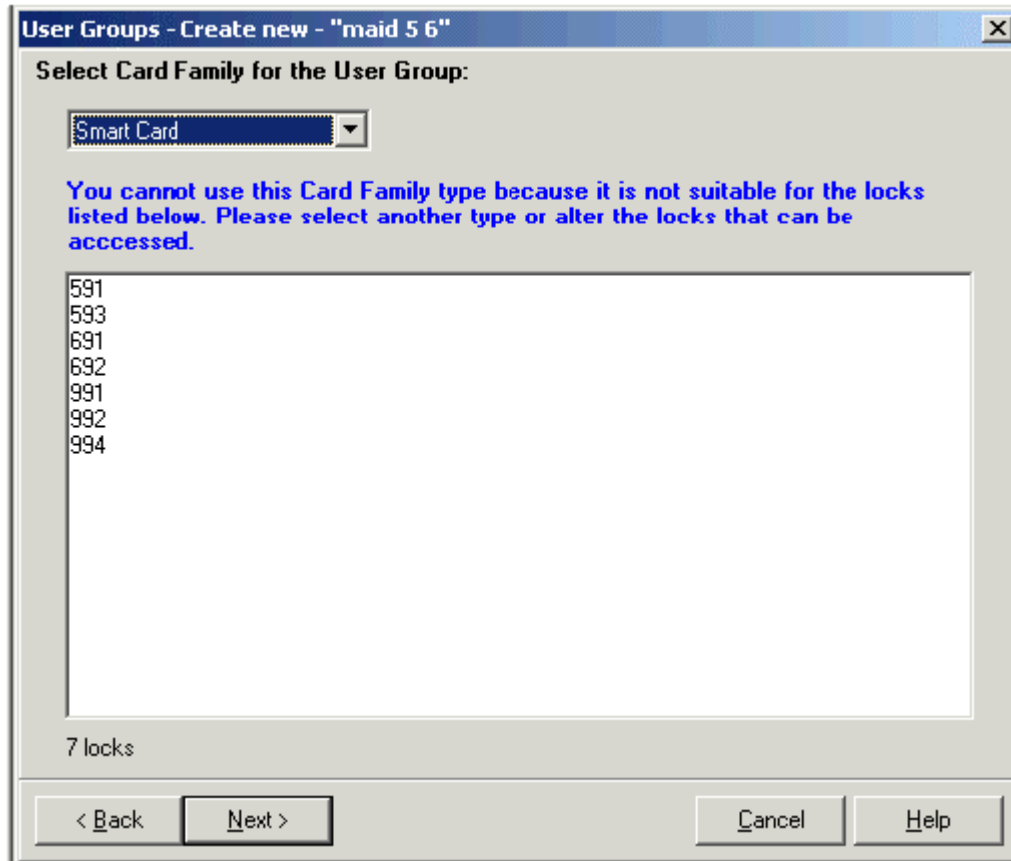
issued. It also allows any PMS interfaces to select the card family without having to provide extra information for each card.



Option	Description
Select Card Family for the User Group	Select the card family type you want to make for this user group Depending on the card family type selected you will be presented with a message telling you whether the selection is acceptable, not acceptable or acceptable with restrictions – see following NOTE for more details.

NOTE

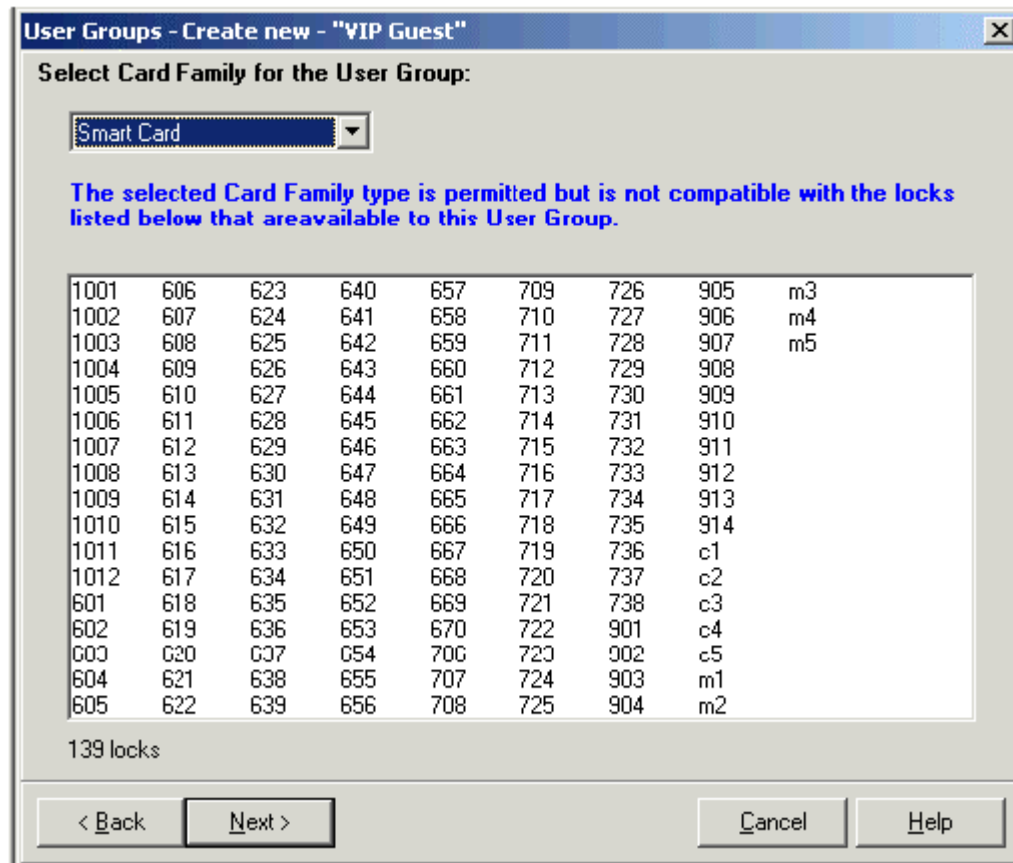
For **Employee Section** User Groups all the locks available to the user group must be compatible with the selected card family type. For example, it makes no sense to issue a Smart Card to a maid to clean a set of rooms if some of those rooms only accept mag-stripe cards.



In this case you must reassess the lock / keycard type / usertype setup for the property..

For **Guest Rooms** and **Employee Rooms** the situation is different. When a keycard is made for a member of this type of user group, the room(s) that the keycard will access are selected from a list of all those available. The keycard made will only have access to one (or at most a few) of the total number of available rooms. Therefore, it is not essential that all locks available to the user group accept the card family type selected. Only if an incompatible door is actually selected at card issue time will Vision raise a warning.

For example, let us assume that floor 5 of a property has Da Vinci Combo locks fitted and is intended for use by guests in User Group 'VIP Guest' who will be issued with Smart Cards. The card family type screen might look like this :



The listed locks will not be available to this user group. If one of them is selected at card issue time, Vision will raise a warning.. However, all the Da Vinci combo locks on floor 5 will be available.

User Groups - Results of User Group Wizard

Displays information about the User Group you just created or edited. If there is anything you want to change, you can click the **Back** button and make changes.

User Groups - Change - Regular Guest [X]

The User Group have the following parameters. Click Finish to save new changes to database.

User Group Name: Regular Guest
Deadbolt override: On
Safe access: Off
Reset after cylinder tamper alarm: Off
Audit trail: Off
Time Table: All week
Start Time: 06.08.2002 11:25:55
End Time: 05.08.2004 11:25:55
Card Family Type: Mag Stripe

Common Doors Time Tables

lift 4th floor All week
Parking All week
Fitness Center 07:00-21:00

MACE Hooks

Parking Access

The following Users have System Access for Regular Guest
Front office, Front off supv, Management, VC Supervisor.

< Back Next > Finish Cancel Help

Setting System Parameters



About System Parameters

By setting the System Parameters, you can set all program defaults, which will save steps when using other modules.

It also coordinates settings that you would normally have to go to Windows software to modify.

The Vision Exit Program button is also located in this module.

Users are given access to the Vision system on a module-by-module basis. By locating all of these sensitive functions in the same module, the Vision system protects you from unauthorized changes and from users exiting the program and running unauthorized software.

System Parameters - General screen

System Parameters [X]

LockLink	M200i	PMS - RS232	PMS - TCP/IP	Time-outs	
Time synchronization	Custom	Daylight Savings	Autobackup	MACE	Workstations
General	Smart Card Options	Check In	Mag Card Encoder	Smart card encoder	

Names

Property name: Pines Hotel

Start day of week: Sunday

Options

Deadbolt Override menu option	<input checked="" type="checkbox"/>
Safe menu option	<input type="checkbox"/>
Override Inhibit	<input type="checkbox"/>
Exit button	<input checked="" type="checkbox"/>
Enable "More Rooms" Tab	<input checked="" type="checkbox"/>
Enable "Name" Tab	<input checked="" type="checkbox"/>

Other

Subtract hours: 2

Issue area: 1

Days to store events: 10

Escape return

Re-lock time (min.): 0

Enabled: ☐

OK Apply Cancel Help

Option	Description
Property Name	The name you enter here will be displayed on the Password screen.
Start Day of Week	All Vision modules that display a calendar will show the first day of the week as Monday unless you select a different day.
Deadbolt Override Menu Option	Determines whether Deadbolt Override will appear as one of the Common Doors options when making keycards. This setting affects guest keycards and employee room keycards only.
Safe Menu Option	Determines whether Safe will appear as one of the Common Doors options when making keycards. This setting affects guest keycards and employee room keycards only.
Override Inhibit	<p>Normally, this is set to "off" which means that when a keycard is used, it invalidates older keycards. Some hotels have situations such as check in desks at airports. This check in stations may not have the latest room availability, so they may want a keycard issued at the hotel to take priority over a keycard made at the airport. In this case, they could set this to "on" at the airport check in station and "off" at the hotel. If two guests were checked into the same room, the keycard made at the hotel would invalidate (override) the one made at the airport.</p> <p>Note that this option would only be necessary if the remote (Airport) check in was using its own copy of the Vision database. If the remote check in was accessing the main Vision database in real-time (the usual case) Override Inhibit would NOT be required.</p>
Exit Button	Click to turn on/off the Exit button that appears on the Main menu. If turned off, it will only be displayed if the user has administrative access.
Enable More Rooms Tab	Click to turn on/off the ability to use 'More Rooms' Functionality in the Guest Cards module. On installation / conversion from Vision 2, this option defaults to 'On'. Switching it 'Off' will hide all the 'More Rooms' screens in the Guest Cards and Employee Rooms modules, effectively disabling the functionality from the user interface (Note : the more rooms functionality will always be available via the various PMS interfaces, regardless of this setting). Predefined 'Suites' functionality is unaffected by this option.
Enable Name Tab	Click to turn on/off the 'Name' tab in the Guest Keycards and Employee Rooms modules. Unchecking this field will hide the 'Name' tabs in the Guest Keycards and Employee Rooms modules, effectively disabling the functionality from the user interface.
Subtract Hours	<p>This feature allows you to set the time a keycard becomes valid to an earlier time than the Vision system's current time. This setting affects keycards made from all modules.</p> <p>Normally, you will use the Time Synchronization feature to maintain the same time on all workstations. However, the lock time may differ from the time settings on the workstation.</p> <p>Setting a number of hours for this item can prevent any problems that might occur if the time used for the PMS or door locks differ</p>

	from the time used for the Vision system.
Issue Area	<p>If your hotel has more than one check in area, you can assign an Issue Area numbers on a workstation-by-workstation basis. For example, if your hotel has an airport check in, you might want to be able to determine whether a guest was checked in from the hotel or from the airport.</p> <p>When you run Reports or use Verify on a keycard, the Issue Area is included. The number you set here affects only systems using this same database, but you can have more than one workstation with the same Issue Area number.</p>
Days to store events	Set the number of days lock events should be stored.
Escape return	<p>Escape Return is a special locking scheme used in certain countries (example : Norway) to meet local fire evacuation requirements. If Escape Return is enabled, all guest keycards will be made with two mag-stripes – one to open the door and the other to close it.</p> <p>You can only use Escape Return if your Hotel is fitted with locks that are compatible with the special Escape Return requirements. Contact your VingCard supplier for details.</p> <p>To set the number of minutes for Re-lock time you first need to check the Enable box. Enabling escape return means that:</p> <p>If a lock is unlocked by the open stripe on a card, the lock unlocks/re-locks as a standard lock.</p> <p>If a lock is opened from the inside, the re-lock timer starts, and when it expires the lock is locked. To force the locking before the timer expires, you need to use the close stripe on the card.</p> <p>You can set a Re-lock time between 0 and 30 minutes. If you set the value to 0 minutes, the door will stay open until the door is locked using the deadbolt or the close stripe on the card.</p>

System Parameters - Check In Screen

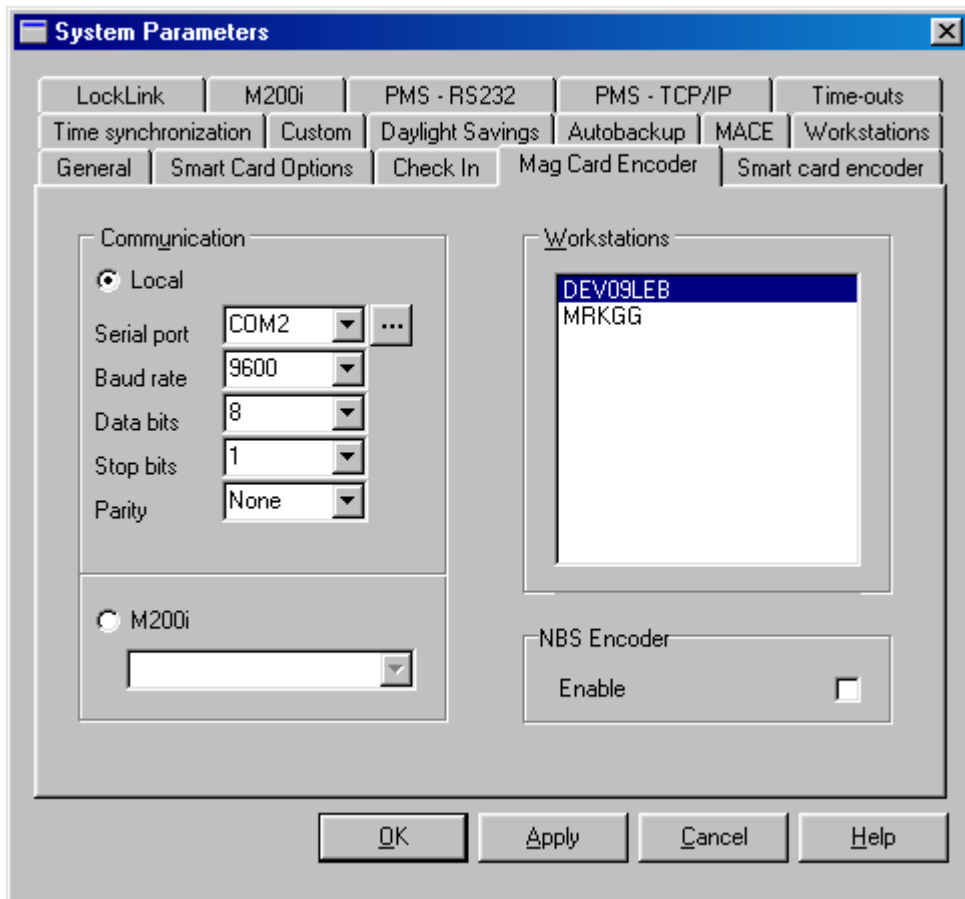
Items on this screen set defaults for the Guest Keycards and Employee Rooms modules.

Option	Description
User Group	All options on this screen will be set up for this User Group
Section (Keycard Type)	Determines which pre-defined Type will be associated with keycards made for this User Group
Check In Time	Determines the Time that will used as the default for check in. If set to 00:00, the current time will be used. This time is based on a 24-hour clock.
Check Out Time	Determines the Time that will be used as the default expiration time of the keycard. If set to 00:00, the same time of the day as "Check In Time" will be used. This time is based on a 24-hour clock.
Length of Stay	Determines the number of days that will be used as default for length of stay (guests).
Length of Stay Empl. Rooms	Determines the number of days that will be used as default for length of stay when an employee rooms card is made.

System Parameters – Mag Stripe Encoder Screen

Vision allows you to set a default mag-stripe and a default smart card encoder for each PC running Vision.

Items on this screen control the Mag Stripe Encoder settings for each PC.



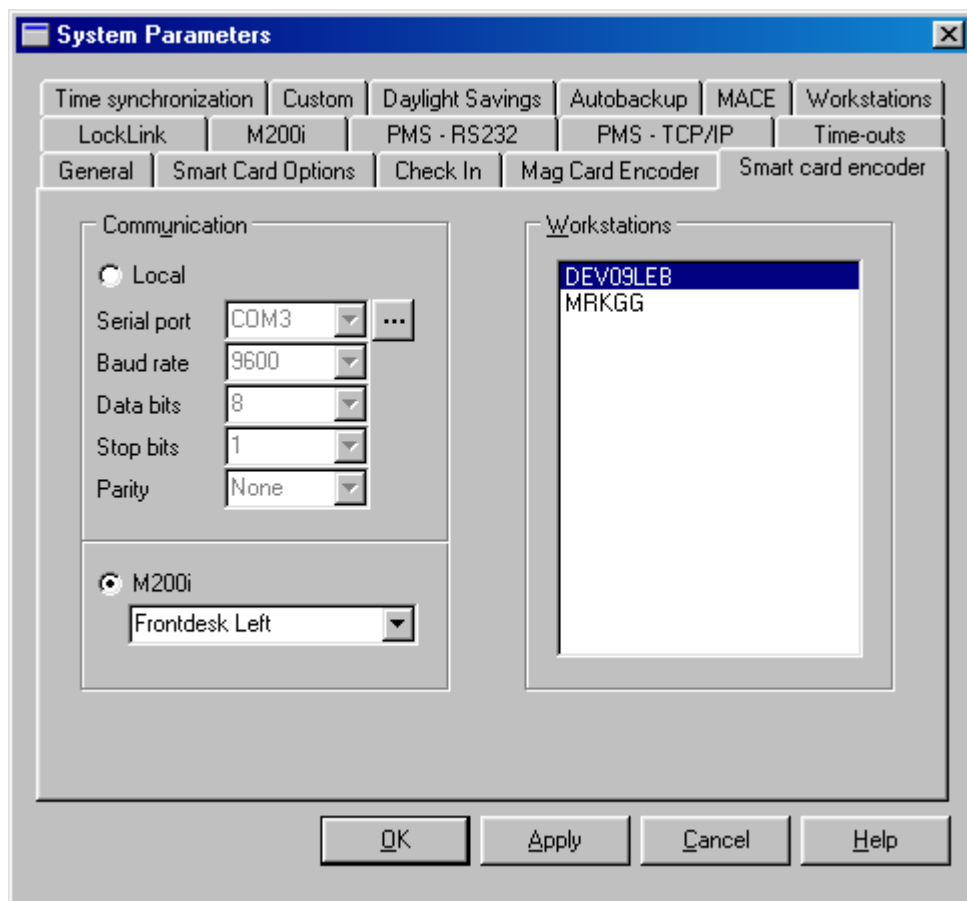
Option	Description
Workstations	Determines which workstation you are currently setting parameters for.
Serial Port	Specifies the Encoder com port for the selected workstation. Click on the serial port button to display a drop-down list that shows the current settings for each Com port on the workstation
Baud Rate	The baud rate must conform to the Encoder for the selected workstation.
Data bits	This must conform to the Encoder for the selected workstation and is usually set to 8.

Stop bits	This must conform to the Encoder for the selected workstation and is usually set to 1.
Parity	This must conform to the Encoder for the selected workstation and is usually set to NONE.
M200i	Specifies that the cards will be encoded on the selected network encoder (M200i), for the selected workstation. The drop-down list shows all available M200i units.
NBS Encoder	Enables communication with an NBS style encoder. See Chapter 10 of the Manual for further details on using NBS encoders.

System Parameters – Smart Card Encoder Screen

Vision allows you to set a default mag-stripe and a default smart card encoder for each PC running Vision.

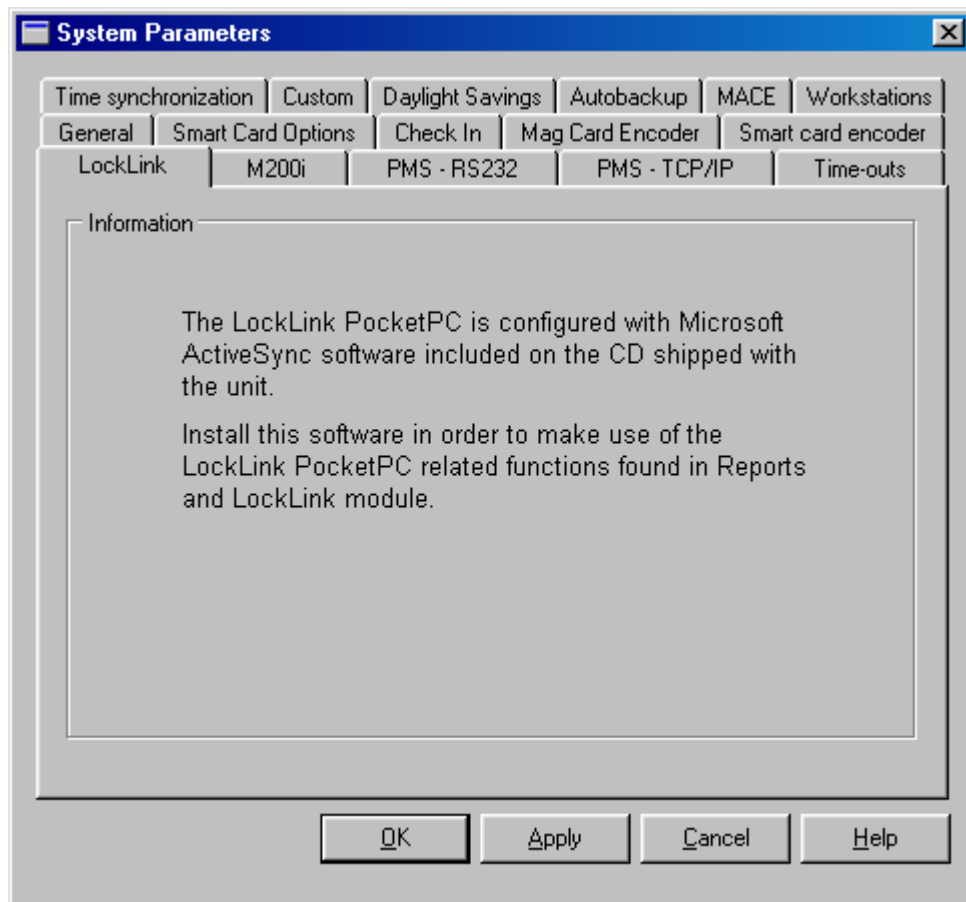
Items on this screen control the Smart Card Encoder settings for each PC.



Option	Description
Workstations	Determines which workstation you are currently setting parameters for.
Serial Port	Specifies the Encoder com port for the selected workstation. Click on the serial port button to display a drop-down list that shows the current settings for each Com port on the workstation
Baud Rate	The baud rate must conform to the Encoder for the selected workstation.
Data bits	This must conform to the Encoder for the selected workstation and is usually set to 8.
Stop bits	This must conform to the Encoder for the selected workstation and is usually set to 1.
Parity	This must conform to the Encoder for the selected workstation and is usually set to NONE.
M200i	Specifies that the cards will be encoded on the selected network encoder (M200i), for the selected workstation. The drop-down list shows all available M200i units.

System Parameters - LockLink screen

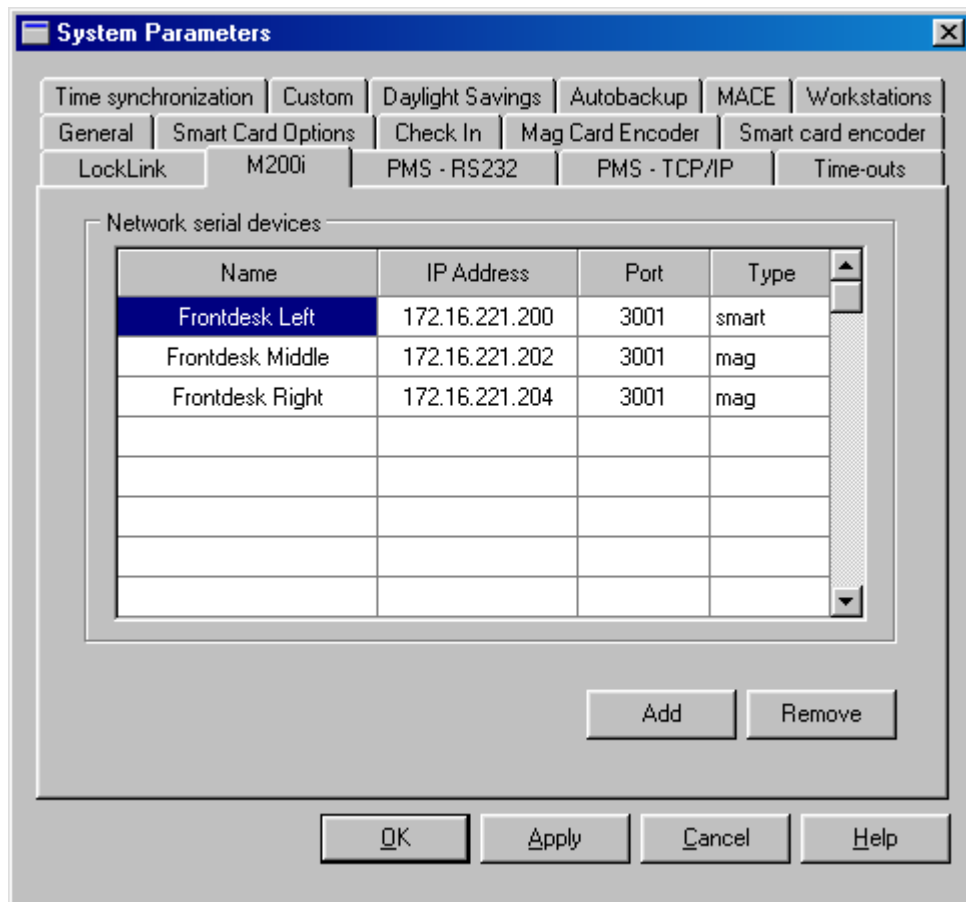
Prior to version 4.0, Vision required serial parameters to be set up for communication with the LockLink. LockLink communication now uses Microsoft ActiveSync so this setup is not required. The following screen simply serves as a reminder to those familiar with older versions of Vision.



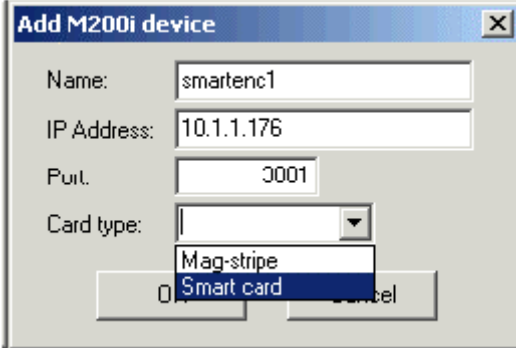
System Parameters - M200i Screen

Items on this screen add, remove or modify the network encoder devices available on the Vision network. Both mag-stripe and Smart Card encoders can be defined here.

Note that the name 'M200i' refers to a type of Ethernet to RS232 Serial Server used in many Vision installations to connect encoders to the Vision network.



Column	Description
Name	The name of this device setting.
IP Address	The IP address of the device you are setting up.
Port	The port name that you are accessing the device from.
Type	Mag-stripe or Smart encoder

Button	Description
Add	<p>Adds a new M200i device to database. The dialog box will prompt for data.</p> 
Remove	Deletes currently selected M200i device from VISION database.

NOTE: To modify an individual setting, double click on it and type the new information.

System Parameters – PMS – RS232 screen

Items on this screen control the Property Management Software (PMS) settings for the workstation connected to the PMS system via an RS232 cable connection. The PMS Interface is also turned on/off from this screen.

The screenshot shows the 'System Parameters' dialog box with the 'PMS - RS232' tab selected. The dialog has a title bar with a close button. Below the title bar is a row of tabs: 'Time synchronization', 'Custom', 'Daylight Savings', 'Autobackup', 'MACE', 'Workstations', 'General', 'Smart Card Options', 'Check In', 'Mag Card Encoder', 'Smart card encoder', 'LockLink', 'M200i', 'PMS - RS232' (selected), 'PMS - TCP/IP', and 'Time-outs'. The main content area is divided into several sections. At the top, there is a checkbox for 'PMS enabled' which is checked, followed by 'Current status: Not Running' and a 'Start PMS' button. Below this is a 'Communication' section with dropdown menus for 'Serial port' (set to COM2), 'Baud rate' (set to 9600), 'Data bits' (set to 8), 'Stop bits' (set to 1), and 'Parity' (set to None). To the right of the 'Communication' section is an 'Other' section with a 'Show debug window' checkbox (unchecked) and an 'Address mapping' button. Below the 'Other' section is an 'Integration mode' section with four radio buttons: 'Silent' (selected), 'Touch screen', 'Windows', and 'Full Vision'. At the bottom of the main content area is a 'Connection' section with a label 'Workstation connected to PMS' and a dropdown menu showing 'DEV09LEB'. At the very bottom of the dialog are four buttons: 'OK', 'Apply', 'Cancel', and 'Help'.

System Parameters

Time synchronization | Custom | Daylight Savings | Autobackup | MACE | Workstations
General | Smart Card Options | Check In | Mag Card Encoder | Smart card encoder
LockLink | M200i | **PMS - RS232** | PMS - TCP/IP | Time-outs

☒ PMS enabled Current status: Not Running **Start PMS**

Communication

Serial port: COM2
Baud rate: 9600
Data bits: 8
Stop bits: 1
Parity: None

Other

☐ Show debug window
Address mapping


Integration mode

☒ Silent ☐ Touch screen
☐ Windows ☐ Full Vision

Connection

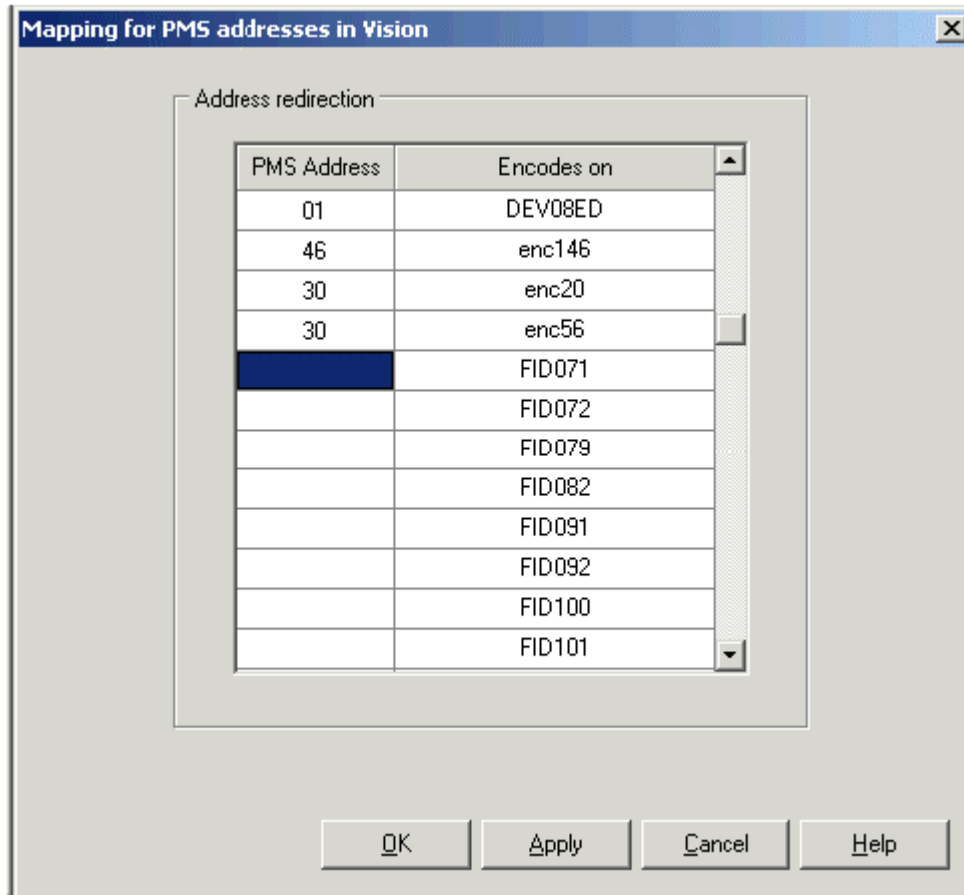
Workstation connected to PMS: DEV09LEB

OK **Apply** **Cancel** **Help**

Option	Description
PMS Enabled	Check this to start the RS232 PMS interface on the selected PC (“Workstation Connected...”) whenever Vision is started.
Current Status	Indicates whether PMS is currently running via RS232 or not.
Start PMS/Stop PMS	This will display as “Start PMS” when the PMS system is not running, and “Stop PMS” when it is. By selecting this, you can turn the PMS interface connection via RS232 on and off.
Serial Port	<p>The com port on the selected PC which will communicate with the PMS. Using this  button allows you to view all the com ports assigned by the Vision system.</p> <p>TIP:</p> <p><i>The list of communication ports that is displayed from the button, always shows 4 com ports.</i></p> <p><i>If your system has more than 4 communication ports, the Vision software will ignore these higher numbers. Therefore, using them with other software will not interfere with the functionality of the Vision system.</i></p>
Baud Rate	The baud rate for the selected port must conform to the PMS system setting.
Data bits	This must conform to the PMS system setting and is usually set to 8.
Stop bits	This must conform to the PMS system setting and is usually set to 1.
Parity	This must conform to the PMS system setting and is usually set to NONE.
Show Debug Window	Used by technical support for troubleshooting.
Address mapping	See Edit Address Mapping , below.
Integration Mode	<p>This selection affects what the user will see when they are encoding a keycard.</p> <p>Silent - The PMS software interface is used. Only the VingCard logo is displayed when running. The only indication to insert a keycard for encoding, is the green light on the encoder.</p> <p>Windows - Windows settings are used to determine how the message to insert a keycard is displayed.</p> <p>Touch Screen - The Guest Keycard Module will appear. Unless they want to change any of the encode settings, all that is necessary is to touch (or click) the Encode button.</p> <p>Full Vision - This is the recommended setting. It integrates with the PMS but also allows the person making keycards to access <i>all</i> of the Vision keycard encoding options.</p>
Workstation Connected to PMS	Name of the workstation that is physically connected to the PMS system.

System Parameters - Edit Address Mapping

PMS address mapping applies to all PMS communication, whether via the RS232, TCP/IP or PMS integration interface methods.



Using this table, a PMS address (numerical) is assigned to each device the PMS system wishes to use to encode cards. A device is either a PC running Vision or a networked encoder (set up using the M200i System Parameters tab). When the PMS requests a keycard to be made it specifies an address. The Vision system examines this address and then uses the information in the address mapping table to decide which device to forward the command to.

The right hand column in the table lists all available devices on the Vision network. The user maps PMS addresses to each required device via the left hand column.

Network encoders will either be mag-stripe or Smart Card types. Therefore, if the PMS sends a command to make a card of a specific card family type (for example mag-stripe or Smart Card, determined by user group), then the addressed device must be compatible. If it is not – for example a request for a Smart Card user group is addressed to a mag stripe encoder – an error will be returned. However, one mag-stripe and one Smart Card network

encoder can be mapped to the same PMS address. In this case (example : address 30 in the screen shot) Vision will examine the user group to determine the required card family type, and make the keycard on the appropriate encoder. In practice therefore, encoders mapped to the same address should be physically in the same location.

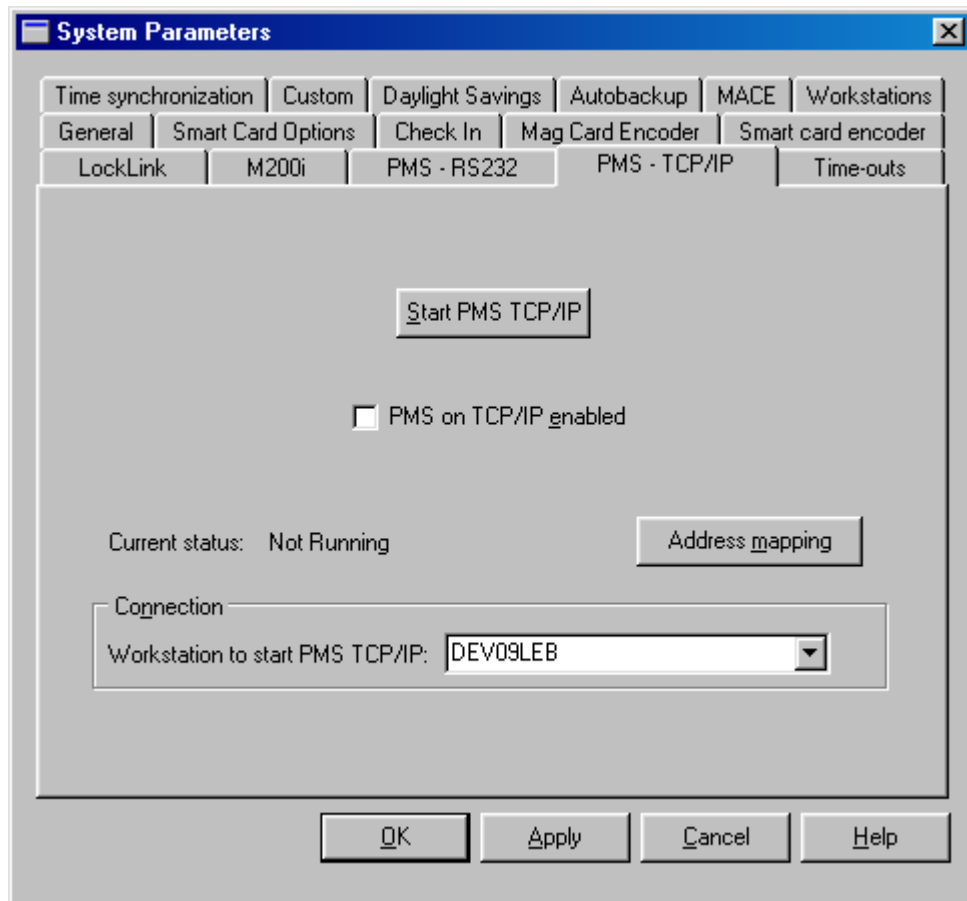
PCs running Vision can each have a default mag-stripe encoder and a default Smart Card encoder, each set up by the appropriate System Parameters tab. PMS commands sent to addresses that map to a PC (example : address 01 in the screen shot maps to PC DEV08ED) will cause keycards to be made on the appropriate default encoder for the PC. Whether a mag-stripe or Smart Card is made depends on the User Group sent by the PMS. If there is no default encoder of the appropriate type an error will be returned to the PMS.

Option	Description
PMS address	Any value from 0 to 99 or empty. You can legitimately use the same address for one mag-stripe and one Smart Card network encoder.
Encodes on	Name of the unit. This column is read only , so the data cannot be changed. All VISION PCs on the network will be listed, as well as network encoders defined on the "System Parameters – M200i" screen.

NOTE: To remove an address, double click on it and then type any invalid character (such as a letter instead of a number).

System Parameters – PMS – TCP/IP screen

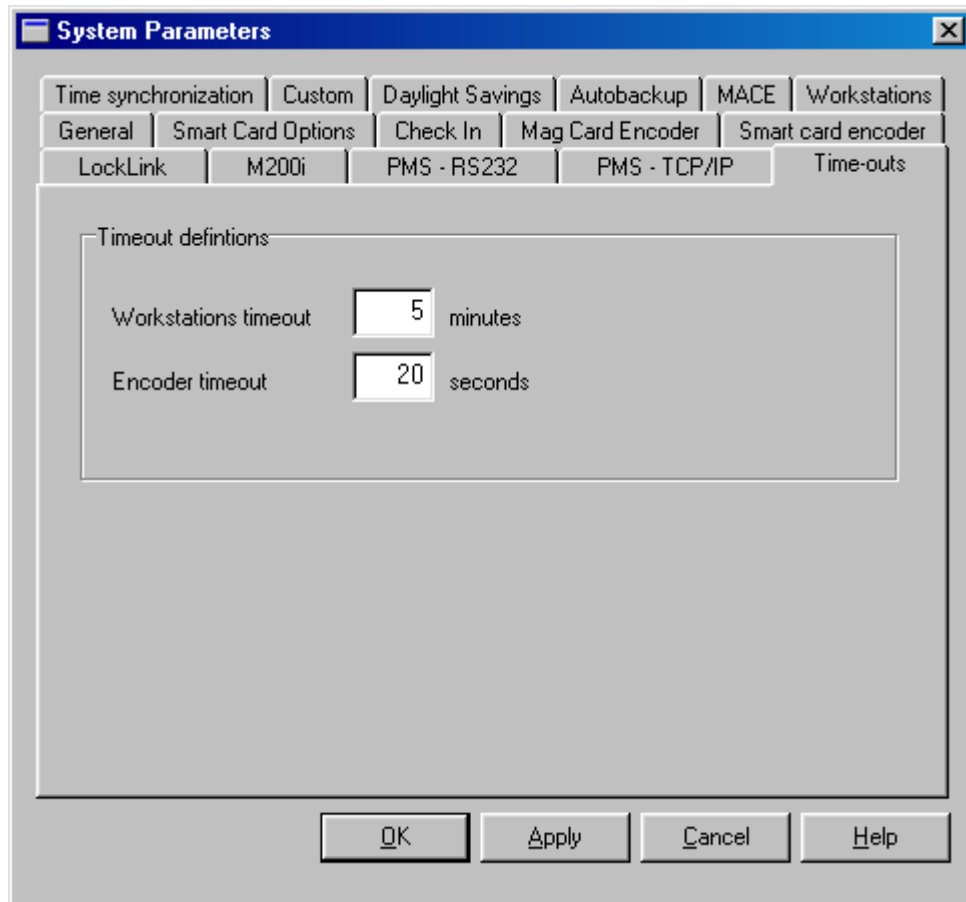
Items on this screen control the Property Management Software (PMS) settings for PMS interfaces that use TCP/IP. The PMS TCP/IP Interface is also turned on/off from this screen.



Option	Description
Start/Stop PMS TCP/IP	Starts/Stops the Vision TCP Client Link (VTCLink) program which enables the PMS to connect to Vision via TCP/IP.
PMS on TCP/IP enabled	Check this to start VTCLink PMS on the selected PC ("Workstation to start...") whenever Vision is started.
Current Status	Indicates whether VTCLink is currently running or not.
Address mapping	See Edit Address Mapping section for PMS RS232 on previous page. The address mapping for RS232 and TCP/IP is exactly the same – you can just access it from two different places.
Workstation to start PMS TCP/IP	Name of the workstation which runs the PMS TCP/IP VTCLink program – which handles and redistributes the TCP/IP messages from the PMS in line with the address mapping information.

System Parameters - Time-outs screen

This screen determines how long the system will wait when there is no activity, before returning users to the Login screen. It also allows you to set the amount of time to wait for a keycard to be encoded.



Option	Description
Workstations Timeout	Determines how many minutes the system will wait before returning to the login screen.
Encoder Timeout	Specify how many seconds you want the system to wait if the encoder is not working or if a keycard is not inserted.

System Parameters - Time Synchronization

Use this screen to turn on the option to automatically update the clock time settings for all workstations. If you use this option you will need to designate which workstation's time setting you want to use as a basis for determining what time to set the others to.

NOTE: It is not uncommon for a computer clock to gain or loose time, so it is recommended that you use this option if you have more than one check in station. Keep in mind that the time on the keycard is read by the locks to determine when a keycard expires. Also newer guest keycards will invalidate older keycards, so it is important that when there is more than one workstation, they are all set to the same time.

Option	Description
Enable Vision Time Synchronization	If you do not check this box, the time in the workstations will not be updated automatically.
Master Time Control Station	Select which workstation's clock to use as a basis for resetting the clock in other systems.
Time of Day to Sync(hronize)	The synchronization will take place daily. Select a time of day that you want it to occur. TIP: The update can occur without interrupting use of the Vision

	system. Choose a time when you expect the network to be running.
--	--

System Parameters - Custom Screen

System Parameters

General | Smart Card Options | Check In | Mag Card Encoder | Smart card encoder
 LockLink | M200i | PMS - RS232 | PMS - TCP/IP | Time-outs
 Time synchronization | **Custom** | Daylight Savings | Autobackup | MACE | Workstations

Track info

Track #1 enabled ☒

Info on track #1
 PINES HOTEL

Track #2 enabled ☐

Info on track #2

Track #1 and #2 follow the ANSI/ISO standard for encoding and character set.
 Track #1 supports max. 76 characters, track #2 max. 37 characters.
 Start/end sentinels and LRC are generated automatically.

OK Apply Cancel Help

Use this screen if you want to enter fixed information to be placed on tracks 1 and/or 2 during encoding. You will need multi track encoders for this feature to work.

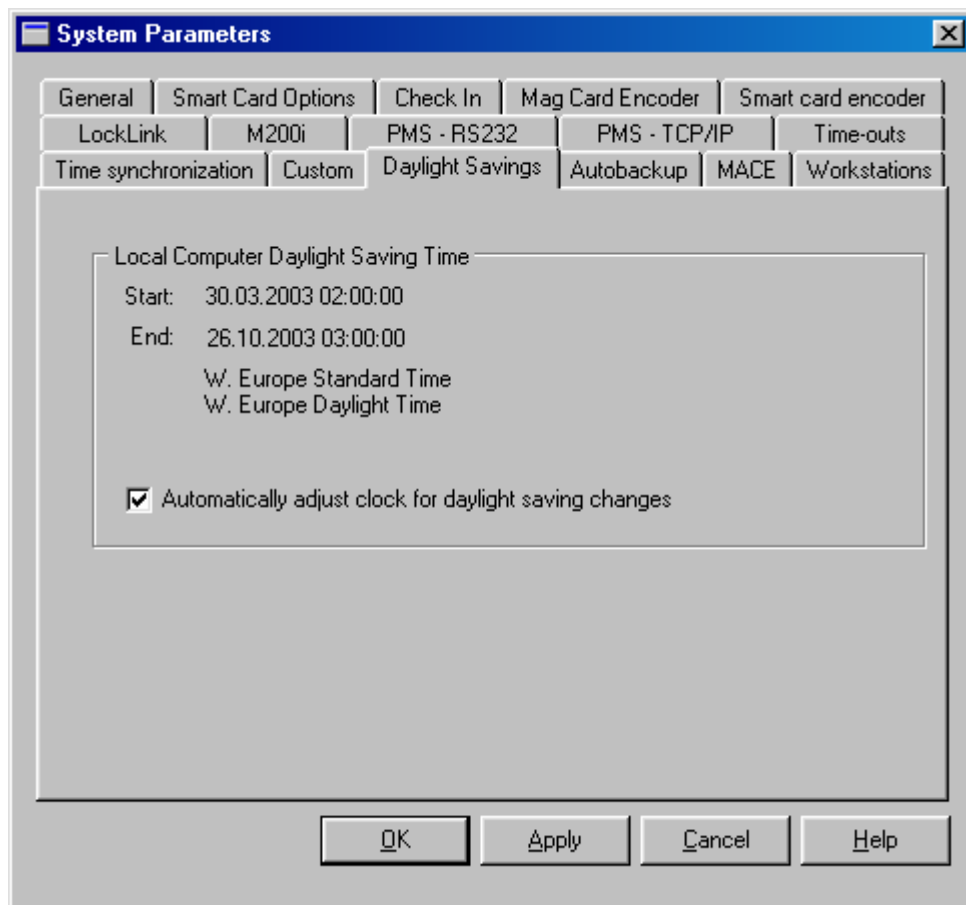
NOTE: If you are using Vision to encode data sent by the PMS system on either of these tracks, the PMS data will be encoded and the data you enter on this screen will be ignored.

Option	Description
Track #1 Enabled	Box must contain a check mark to enable this feature.
Info on Track #1	Up to 76 alpha numeric characters compliant the ISO 3554 standards.
Track #2 Enabled	Box must contain a check mark to enable this feature.

Info on Track #2	Up to 37 numeric characters compliant with the ISO 3554 standards.

NOTE: The encoding of data on tracks 1 and 2 follows ISO/ANSI standards which specify that a start sentinel be used to mark the start of the data and a Low Redundancy Checksum (LRC) is used after the end sentinel. Most encoders add this automatically, but some do not. Regardless of which encoder you use, you will not need to enter the start/end sentinels, as the Vision system will manage this for you.

System Parameters - Daylight Savings screen



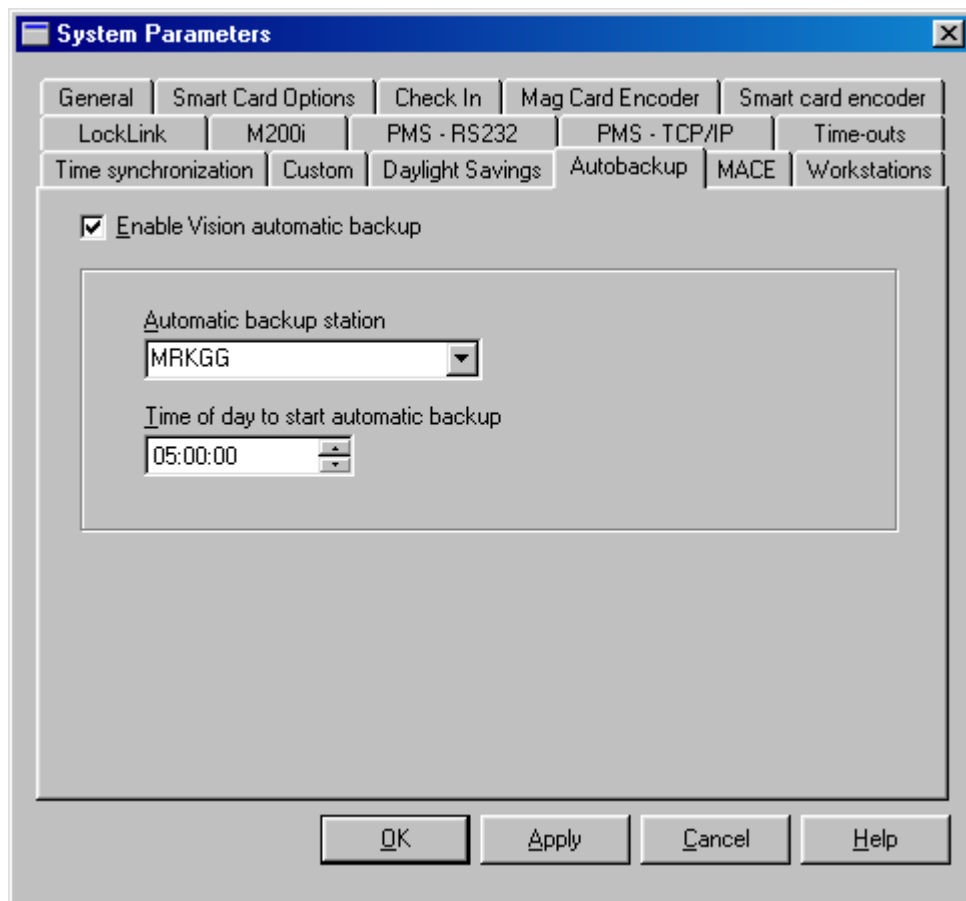
This screen shows the current settings for daylight savings time. The Vision system gets this information from Windows. You can check or uncheck the option “Automatically adjust clock for daylight saving changes”.

This information is used by the LockLink to program all locks so that they will also change time if Daylight Savings Time is used.

To select a different time zone, use Windows settings

System Parameters – Autobackup screen

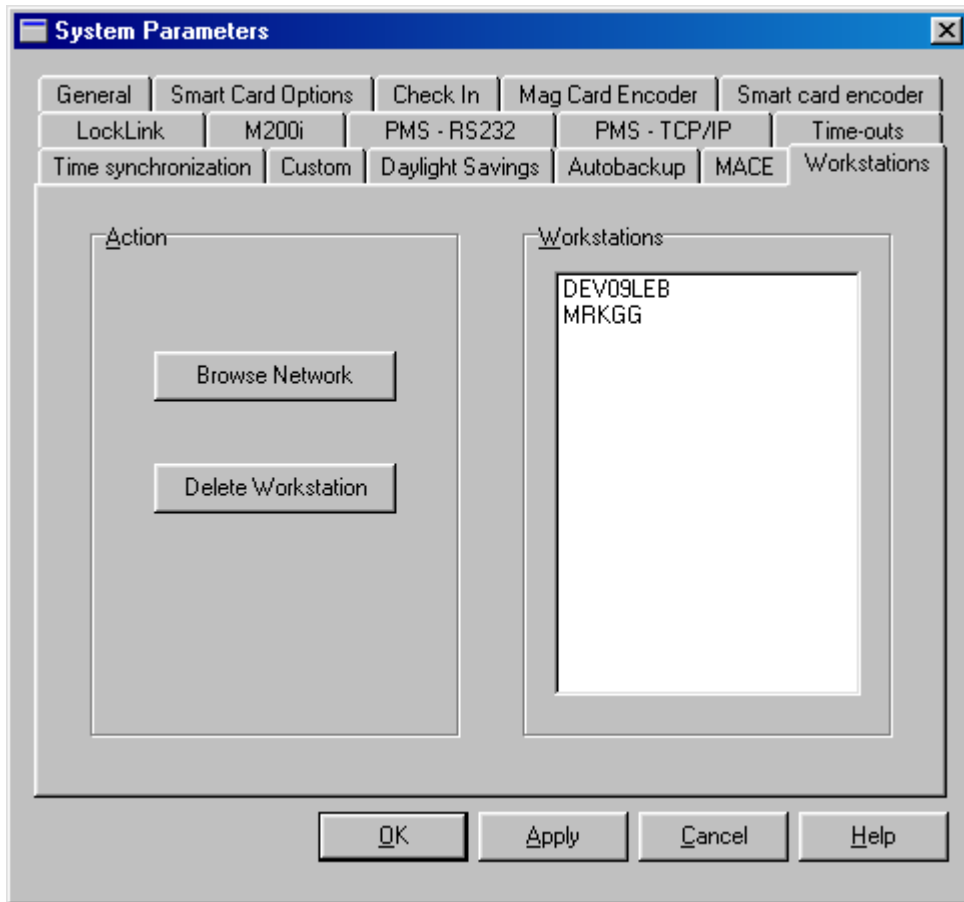
On this screen, you enable or disable the Vision automatic backup feature. With the autobackup feature enabled, all Vision data will be backed up automatically every day at the selected time. You can continue to use Vision on other PCs throughout the backup process. If you should ever need to restore a backup, please refer to the documentation for the Vision Backup module where the Unpack and Restore process is described.



Option	Description
Enable Vision automatic backup	Click to check or uncheck the option to enable or disable the autobackup feature.
Automatic backup station	Select the Vision PC to be initiate the backup (This should generally be the server).
Time of day to start automatic backup	Set the time for the autobackup to start.

System Parameters – Workstations screen

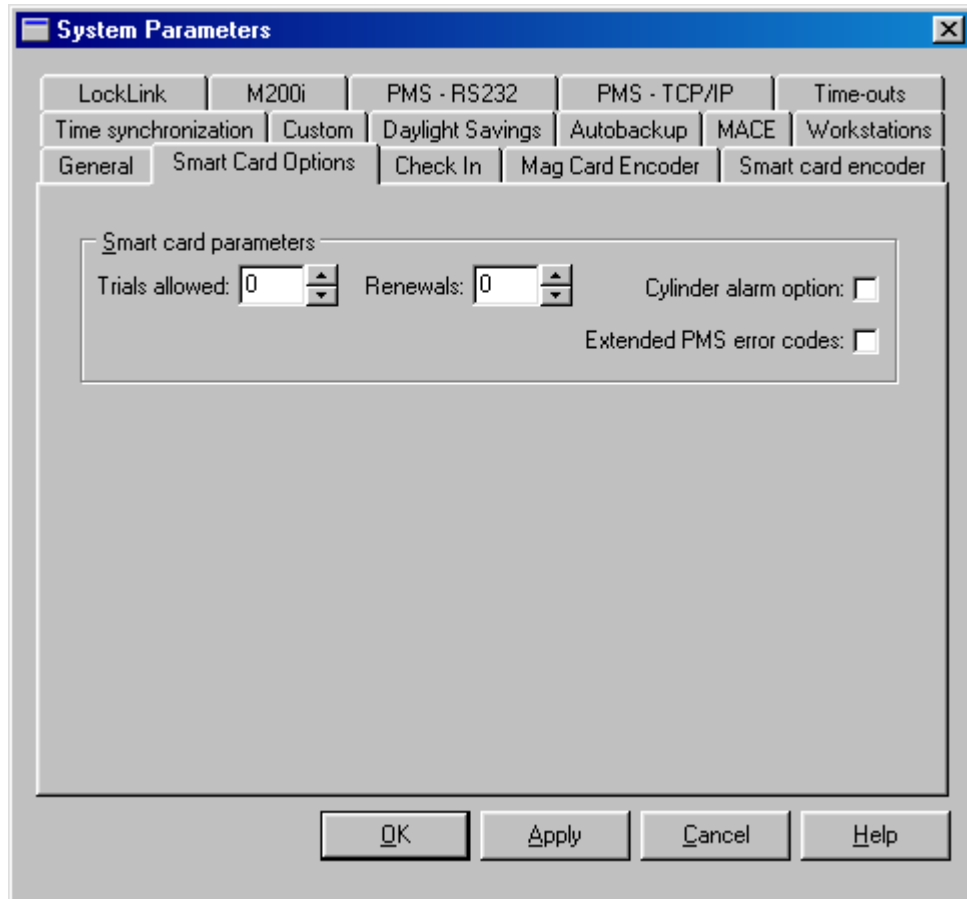
Use this screen to search the network for Vision workstations, and to delete inactive workstations from the Vision database.



Option	Description
Browse Network	Click to browse the network for PCs running Vision.
Delete Workstation	Click to delete the selected PC from the Vision database. Note that if you delete a PC that is not currently running Vision, it will be re-registered in the Vision database. That is, deleting does not cause PCs to be permanently 'lost'. You should delete PCs that were once connected but will not be again : notebooks used for testing etc.
Workstations	Displays all PCs registered in the Vision database.

System Parameters – Smartcard options screen

Use this screen to set parameters relevant for installations where Smartcards are used.



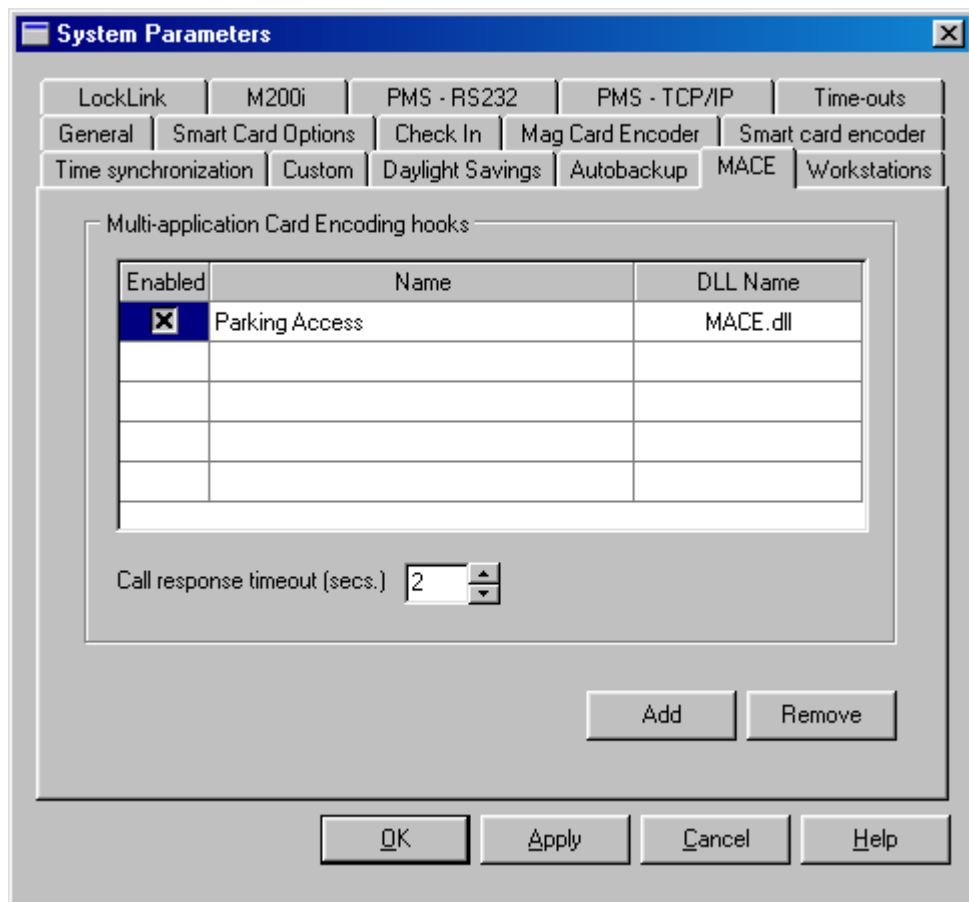
Option	Description
Trials Allowed	<p>Trials Allowed and Renewals are the initial values of counters written to each Smart Card made. Their purpose is to prevent someone that finds a Smartcard repeatedly trying it in doors until they find a door that opens.</p> <p>The Trials Allowed counter is decremented each time a Smartcard is used in an invalid lock (one it has no access rights for). If the count reaches zero, the card is disabled. If the card is used in a valid lock, the count is reset to the initial value specified here.</p>
Renewals	<p>The Renewals counter is decremented each time the 'Trials Allowed' counter is reset. If the Renewals count reaches zero, the card is disabled. When the card is rewritten (for example for the next guest) the count is reset to the initial value specified here.</p> <p>If you do not want your smart cards to ever become disabled due to repeated invalid entry attempts, set both Trials Allowed and Renewals to zero.</p>
Cylinder Alarm Option	<p>VingCard locks with a metal key cylinder raise an alarm if someone tries to use force on the cylinder to open the door. All locks log the alarm to their internal event logs. Locks that accept Smart Cards</p>

	<p>can optionally be set such that, following the alarm, they will flash their light and deny access to all keycards until the lock is reset. In this way, clear and prompt visibility of forced entry attempts can be achieved. The reset occurs when a Smartcard with cylinder alarm override rights is used in the lock. Cylinder alarm override rights are set per User group.</p> <p>If you want to Smartcard locks to behave this way following a cylinder alarm., check this option. The option is universal – it will apply to ALL Smartcard locks at your property.</p>
Extended PMS error codes	<p>Vision is capable of generating some new, detailed PMS error codes that were not present in Vision 3.1 and earlier.</p> <p>Check this option to allow Vision to send these new error codes. If you leave it unchecked the codes will be replaced with an error code 1 – 'Unspecified error'. This allows Vision to be backwards compatible with PMS software not updated to interpret the new codes. See Manual PMS Chapter for more details.</p>

System Parameters – Hooks screen

You may encode up to three tracks on a magnetic card. Vision and VingCard locks use track 3. You may set up Vision to write static data on track 1 and 2 for all guest keycards made by the system. Alternatively, an interfaced PMS may specify track 1 and track 2 data. However, neither of these methods is suitable if you need to construct specific information for the tracks on a per guest approach.

If you need guest-specific data to be written to tracks 1 or 2, Vision can use a “Multi-application Card Encoding plug-in” (“MACE plug-in” or “MACE hooks”). Examples of guest specific data might be data relating to Parking or Room Safes. A MACE plug-in is basically a dynamic link library (DLL).



Option	Description
Add	Press this to add a MACE Plug-in to the Vision system. You will be presented with a browse window. Browse to and select your MACE Plug-in DLL. This DLL must be compatible with VingCard requirements. See MACE Manual for full details.
Remove	Remove the link between Vision and the MACE Plug-in. This does NOT delete the actual DLL file.

Enabled	The ability to allow a particular hook to encode on a keycard is set up per user group – in a similar way to Common doors. However, the hook will never be available – even if specified for a particular user group - unless enabled here. If enabled is not checked, the hook is completely disabled – that is, known to the Vision system but not used.
Name	After adding a MACE DLL, double click here and enter a meaningful name. Examples: Parking Hook; Room Safe hook.
DLL Name	The file name of the DLL. Not editable. For information only.
Call Response Timeout	The time a function in the DLL has to respond after being called by Vision. If no reply is received within this time, Vision will continue standard operation – See Vision Manual for full details.

Setting System Access

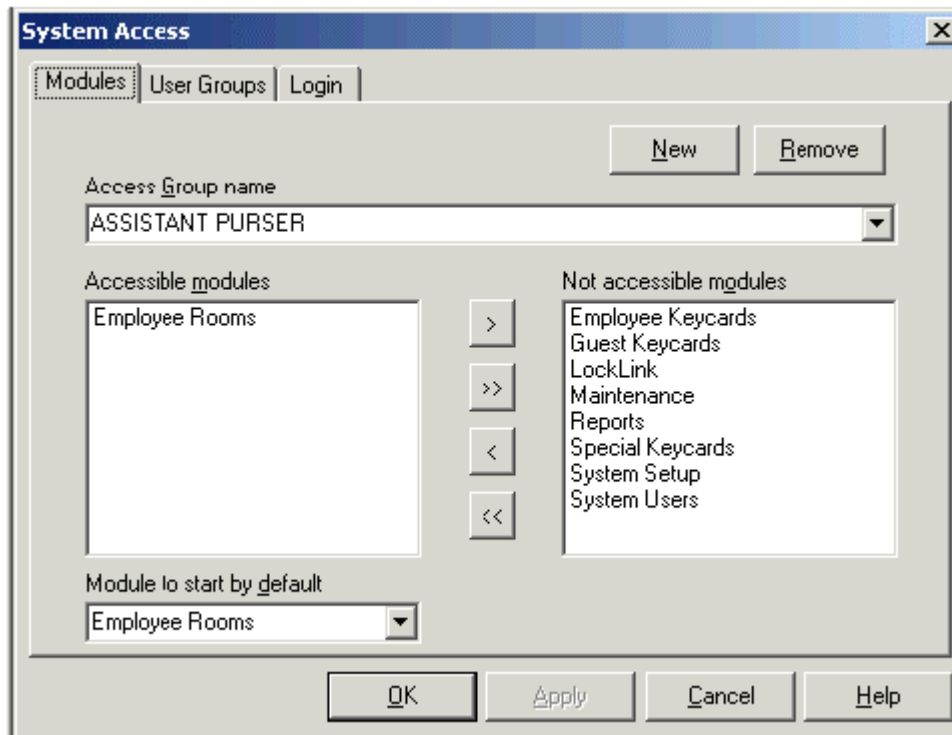


About System Access

System Access settings allow you to set up Access groups (relating to groups of staff that will use Vision) and assign to each access group :

- the Vision modules that access group members can use
- the User Groups that access group members are authorized to work with (for example, issue cards to)

System Access also allows you to control the level of password protection required for a user to enter and use Vision.

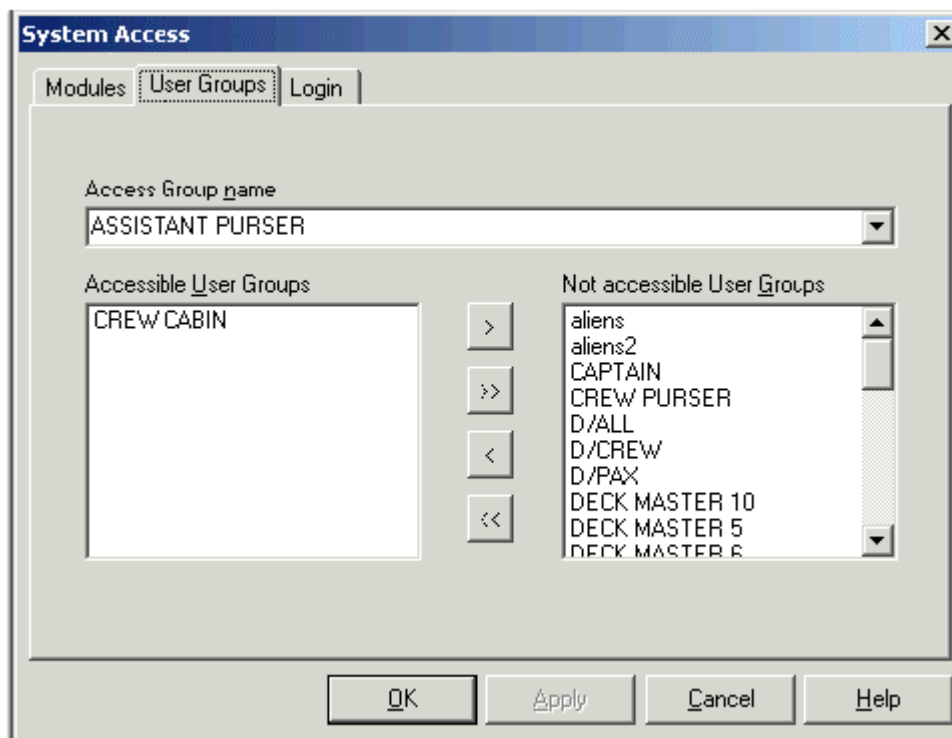


Option	Description
New	Create a New System Access Group
Remove	Remove this System Access Group
(System) Access Group Name	All options on this screen will be set up for this Access Group. Touch the arrow to display the drop-down list of all modules that

	have been installed.
Accessible Modules/Not Accessible Modules	<p>Use the arrow keys between these two windows to control which modules this Access Group will be able to use. The single arrows move one item and the double arrows move all items.</p> <p>Any modules not in the Accessible Modules window will appear greyed out on Main menu screen when users from this Access Group log in.</p>
Module to start by default	<p>Determine the start up module for this Access Group. If you leave this blank, the Main menu will be used as the start-up module.</p> <p>Whenever a user logs in, the system checks to see which module to start, based on the Access Group the user belongs to.</p> <p>For example, you might want the Check In module to start up whenever someone from the Access Group for the front desk logs in.</p>

System Access - User Groups tab

This screen allows you to determine which User Groups each Access Group can make employee keycards for.



Option	Description
Access Group Name	Determines which Access Group you are setting User Groups for. Touch the arrow to display the drop down list
Accessible User Groups/Not Accessible	Use the arrow keys between these two windows to control which User Groups this Access Group will include. The single

User Groups	<p>arrows move one item and the double arrows move all items.</p> <p>When employees choose Add or Change in the Employee Keycards module, the only employee names that will be listed are those that match the Accessible User Groups window of this screen.</p> <p>If you do not want the employees in this Access Group to be able to issue employee keycards, leave the Accessible User Groups window empty.</p>
--------------------	---

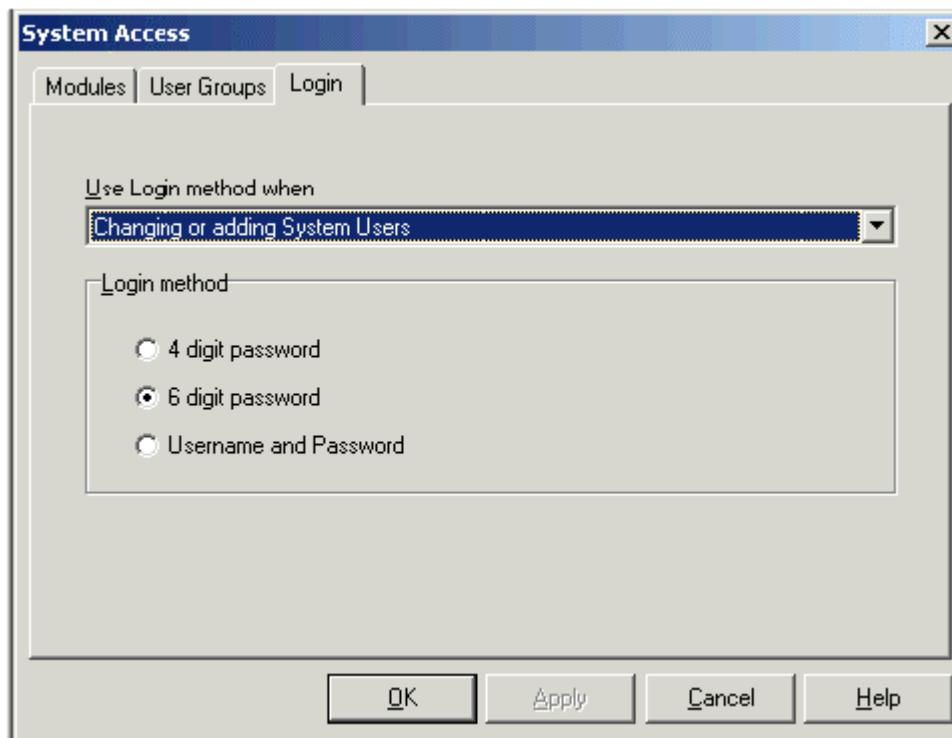
System Access – Login tab

Vision allows you to select from 3 levels of password protection :

- a 4 digit PIN code (as per previous Vision versions)
- a 6 digit PIN code
- Username and Password (similar to Windows)

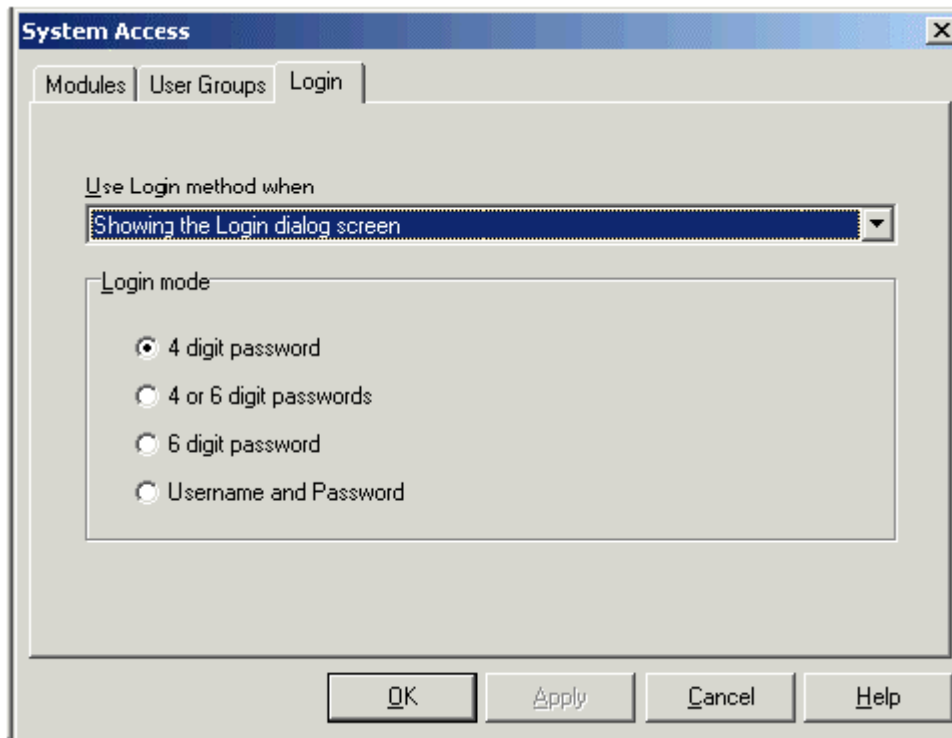
There is a drop down box “**Use Login method when**” (see screen shot)

If you select “**Changing or adding System Users**” you define the type of password that will be assigned to any new system users you define (using the System users module).



Option	Description
4 digit password	New users will be assigned an automatically generated 4 digit password.
6 digit password	New users will be assigned an automatically generated 6 digit password.
Username and Password	New users can select their own unique, alphanumeric Username and Password. (Only the Password will be case sensitive).

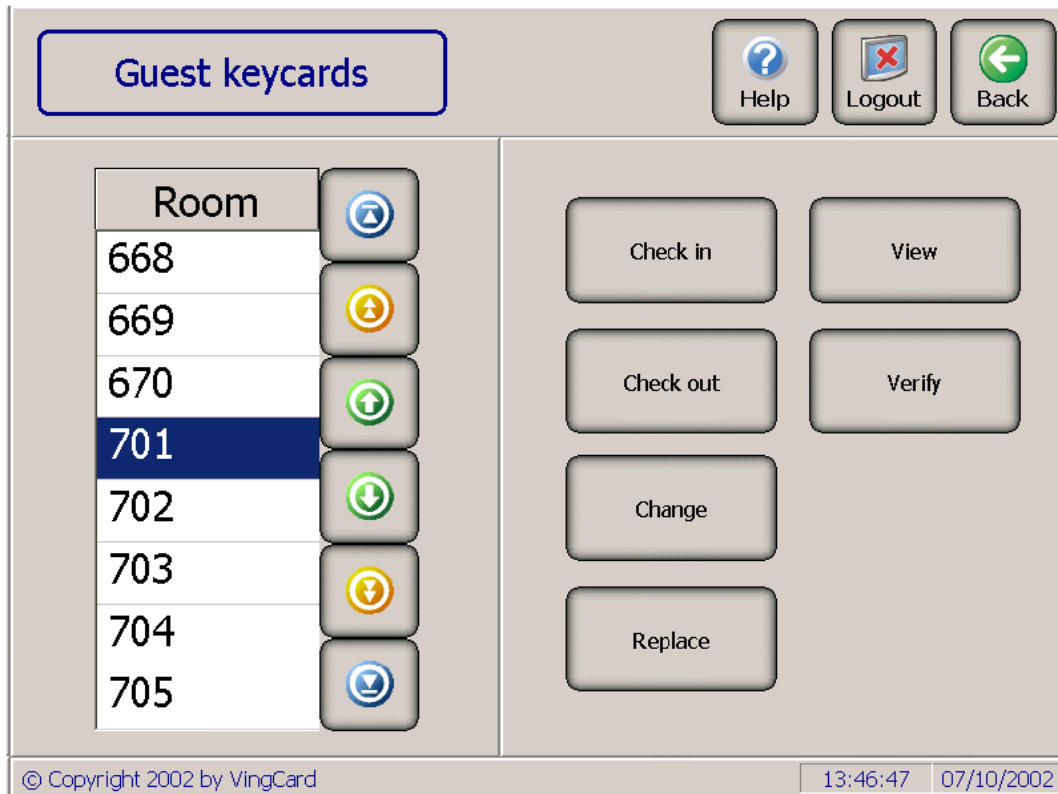
If you select “**Showing the Login dialog screen**” you define the level of password that will be required to enter the system at the Login screen.



Option	Description
4 digit password	All users must log in with a 4 digit password
6 digit password	All users must log in with a 6 digit password
4 or 6 digit password	Users may log in with a 4 or a 6 digit password. This option allows an easy upgrade from 4 to 6 digit passwords. Existing 4 digit users can still log in whilst new users are assigned and use 6 digit passwords. Eventually, each 4 digit user can have their password upgraded using the System Users module.
Username and Password	All users must log in with Username and Password. Note : This option allows an easy upgrade from 4 or 6 digit passwords to username and password. Existing 4 / 6 digit users can still log in whilst new users are assigned and use usernames and passwords. The 4 / 6 digit users can log in by leaving username blank and entering their 4 / 6 digit code as the password. Eventually, each 4 / 6 digit user can have a username and password assigned using the System Users module.

Guest Keycards Module





What the Guest Keycards Module Does

You can use the Guest Keycards module to perform any of these tasks:

- Check in/pre-register a guest
- Check out a guest
- Change a keycard
- Make duplicate guest keycards
- Replace lost or stolen guest keycards
- Verify (read) the information on a guest keycard

Quick Guide to Using the Guest Keycards Module

This topic was designed as a quick reference. For more details on each task, touch the **Help** button and select the appropriate Help topic.

Task	Beginning from the Check in screen:
Check In/Pre-register Guests	<ul style="list-style-type: none"> • Enter Room Number • If the card is for a suite (connecting rooms) touch the type button and select correct suite. • Touch the Name tab and enter guest name. • Touch the More rooms tab and enter room numbers, if making a keycard valid for more than one room • Select check in/out dates and times.

	<ul style="list-style-type: none"> • Change Common Door options if required • Select Name tab and enter guest name if required • Touch the More rooms tab and enter room numbers, if making a keycard valid for more than one room • Touch Encode • Choose Make new if a popup appears indicating room is occupied
Adding guests to a room (Duplicate keys)	<ul style="list-style-type: none"> • Enter Room Number (and appropriate 'more rooms' numbers) • If the card is for a suite (connecting rooms) touch the type button and select correct suite. • Select Name tab and enter new guest name if required • Touch Encode • Select Copy Old from popup
Replace Guest Keycards	<ul style="list-style-type: none"> • Touch Back • Choose a Room number • Touch Replace • If a list of cards is shown, select the card you want to replace (refer to dates, name tab etc) • Touch Encode
Check Out Guest	<ul style="list-style-type: none"> • Touch Back • Choose a Room number • Touch Check out • If a list of cards is shown, select the card you want to replace (refer to dates, name tab etc) • Touch Remove
View Guest Keycards for a room	<ul style="list-style-type: none"> • Touch Back • Choose a Room number • Touch View • Enter room number and touch Find to view other rooms

Verify Guest Keycard	<ul style="list-style-type: none">• Touch Back• Touch Verify• Insert keycard when prompted• Touch Verify to verify additional keycards
----------------------	---

Checking in/Pre-registering Guests

About Checking in/Pre-registering Guests

The Vision system allows each hotel to customize Check In to meet their needs. Therefore, some of the Check In options will vary depending on the decisions your hotel made:

- **Connecting rooms** – If your hotel has set up the Vision system with connecting rooms, you will be able to assign them to guests at check in.
- **Guest name** – If you wish, you can enter guest names when checking in a guest. This option can be disabled via Setup.
- **More rooms** – If the guest rents more than one room or is allowed access to more than one guest room, and the rooms are not defined as connecting rooms, you can use the More rooms tab. Here you can enter the numbers of up to two rooms the keycard you make will be able to open. This option can be disabled via Setup.
- **User Groups** – Whenever you check in a guest, you must select a User Group for them. Different User Groups have different access privileges. For example, your hotel may have a User Group with access to a VIP floor.
- **One-shot Keycards** – Normally, hotels will use the Employee Rooms module to make these keycards which can only be used to open a room once. See the Employee Rooms Help system for details.
- **Common Doors** – In addition to the access controlled by the User Group, you can give a guest access to other doors and locks, or give the guest Deadbolt Override access to their room. Each hotel sets up these selections.
- **NOTE:** If you are unsure of how your hotel uses any of these options, check with your hotel's Vision system administrator.

How to Check in / Pre-register a Guest for a single room

1. If the Check In screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, then select **Guest Keycards**.
2. Make sure that the **Room** tab is selected. If the correct room number is not already selected, use the number pad on the right side of the screen to enter the number of the guest room.

TIP: *A to Z characters in room numbers* - The keypad includes only numbers, so if your hotel has room numbers such as S201, use the following method to select the room number from a list:

*From the Check In screen, touch **Back** to display the **Guest Keycards** menu screen.
Choose the correct room number from the list, and then touch **Check In** to return to the **Check In** screen.*

3. If you want to enter the guest name, touch the **Name** tab and enter the guest's **first** and **last name**.
4. If the guest requires to have access to more than one guest room and the rooms are not defined as Connecting rooms, touch the **More rooms** tab. Enter the room numbers of up to four rooms the keycard should be able to open in addition to the room number you entered on **Room** tab.
5. To change the **From/Until Date**, touch the displayed date and then touch the correct date that appears on the right side of the screen.
6. To change the **From/Until Time**, touch the displayed time and then touch the position on the clock of the time you want to select.
If the AM and PM buttons appear under the clock, you can touch either of

them to switch between AM and PM.

OR

If the 1-12 and 13-24 buttons appear under the clock, you can touch either of them to switch between the first and last 12 hours of the day.

TIP: *To determine whether to display a 12 or 24 hour clock, the Vision system will check to see which Regional Setting your hotel chose from the System Setup module. The two buttons under the clock will either be AM and PM (12:00 PM = Noon) or the first 12 or last 12 hours of the day (24 hour clock).*

7. To change the **User Group**, touch the displayed User Group and then select the correct User Group from the list that appears on the right.

TIP: *A guest user group determines the default privileges for a guest: for example which common doors they can open, what sort of keycard (mag or smart) they will carry. If you are unsure of which User Group to select, see your hotel's Vision System Administrator.*

Touch  or  to move to the **beginning** or **end** of the list.

Touch  or  to move up or down through the list **one screen** at a time.

Touch  or  to move up or down **one item** on the list at a time.

8. If no **Common doors** are currently selected, a “No” will appear for this item. To view the list of selected doors, touch the displayed common doors Yes / No box. Touch any items on the list that appears on the right to select or deselect them.

As well as determining which common doors the guest can open, the list determines whether the keycard will have deadbolt override capability.

The list will also show any Multi-application Card Encoding (MACE) hooks that can write additional information to mag-stripe tracks 1 and or 2. See MACE manual for details of MACE hooks.



TIP: The User Group may have included default access to one or more of the Common Doors. However, you can add or remove access to any items on the Common Doors list.

Making selections from the list:

A red check mark to the left of the list indicates that access will be included with the keycard. Touching items on the list will select or deselect them.

9. To make more than one keycard (Duplicates) for a room or suite, touch the displayed Cards selection and then enter the number of cards using the number pad that appears on the right

TIP: If you wish to tag unique guest names to each card made you should make one card at a time, enter the names for each cardholder on the **Names** tab and select 'Copy Old' after pressing the **Encode** button..

10. When you have finished making all changes, touch the **Encode** button to make the keycard.

TIP: When the new guest uses the keycard to open the room, the previous guest's keycard will no longer open the room door.

For security purposes, the Card Encoder is set to wait for a brief period and if a keycard is not inserted, the process will be cancelled.

11. When you make a new guest keycard, the Vision system checks to see if the current guest keycard has expired. If it has not, you will see a message indicating the room is still occupied. Touch **Make New** to add the first (or only) guest to a room. Select **Copy Old** to add an additional guest to the room.

You will be prompted to insert as many keycards as you requested.

How to Check in a Guest to Connecting Rooms (Suites)

Use these instructions if the Vision system for your hotel has been set up for Connecting rooms (also known as Suites).

1. If the Check In screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Guest Keycards**.
2. Make sure that the **Room** tab is selected. If the correct room number is not already selected, use the number pad on the right side of the screen to enter the **Room Number**.

TIPS: *A to Z characters in room numbers - The keypad includes only numbers, so if your hotel has room numbers such as S201, use the following method to select the room number from a list:*

- From the Check In screen, touch **Back** to display the **Guest Keycards** menu screen.
- Choose the correct room number from the list, and then touch **Check In** to return to the **Check In** screen.

Event Reports and Connecting rooms - Event Reports (Reports module) do not include connecting room information. The only number that will be included in the Event Reports is the number displayed on this screen for Room before selecting the Type button.

3. If the card is for a suite (connecting rooms) touch the **Type** button and select the correct room combination.

4. If the guest requires access to more than the selected Connecting rooms, touch the **More rooms** tab. Enter the room numbers of up to four rooms the keycard should be able to open in addition to the Connecting rooms you already have selected.
5. If you want to enter the guest name, touch the **Name** tab and enter the guest's **first** and **last name**.
6. To change the **From/Until Date**, touch the displayed date and then touch the correct date that appears on the right.

TIP: *Touch the date on the calendar that you want to select as the Check Out date..*

7. To change the **From/Until Time**, touch the displayed time and then touch the position on the clock of the time you want to select.
If the AM and PM buttons appear under the clock, you can touch either of them to switch between AM and PM.
OR
If the 1-12 and 13-24 buttons appear under the clock, you can touch either of them to switch between the first and last 12 hours of the day.

TIP: *To determine whether to display a 12 or 24 hour clock, the Vision system will check to see which Regional Setting your hotel chose from the System Setup module. The two buttons under the clock will either be AM and PM (12:00 PM = Noon) or the first 12 or last 12 hours of the day (24 hour clock).*

8. To change the **User Group**, touch the displayed User Group and then select the correct User Group from the list that appears on the right.

TIP: *The User Group list is set up by each hotel, so this list may change occasionally, and will vary between hotels. If you are unsure of which User Group to select, see your hotel's Vision System Administrator.*

Touch  or  to move to the **beginning** or **end** of the list.

Touch  or  to move up or down through the list **one screen** at a time.

Touch  or  to move up or down **one item** on the list at a time.

9. If no **Common doors** are currently selected, a "No" will appear for this item. To view the list of selected doors, touch the displayed common doors Yes / No box. Touch any item on the list that appears on the right to select or deselect it.

TIP: *The Common Door list is set up by each hotel, so this list may change occasionally, and will vary between hotels. If you are unsure of which Common Doors to select, see your hotel's Vision System Administrator.*

The User Group may have included access to one or more of the Common Doors. However, you can add or remove access to any items on the Common Doors list.

Making selections from the list:

A red check mark to the left of the list indicates that access will be included with the keycard. Touching items on the list will select or deselect them.

- 10.** To make more than one keycard (Duplicates for roommates), touch the displayed **Cards** selection and then enter the number of cards using the number pad that appears on the right.

TIP: *If you wish to tag unique guest names to each card made you should make one card at a time, enter the names for each cardholder on the **Names** tab and select 'Copy Old' after pressing the **Encode** button..*

- 11.** When you have finished making all changes, touch the **Encode** button to make the keycard.

TIP: *For security purposes, the Card Encoder is set to wait for a brief period and if a keycard is not inserted, the process will be cancelled.*

When the new guest uses the keycard to open the room, the previous guest's keycard will no longer open the room door.

- 11.** When you make a new guest keycard, the Vision system checks to see if the current guest keycard has expired. If it has not, you will see a message indicating the room is still occupied. Touch **Make New** to add the first (or only) guest to a room. Select **Copy Old** to add an additional guest to the room.

You will be prompted to insert as many keycards as you requested.

<p>NOTE: After a few minutes of inactivity, the Login screen will be displayed and you will need to re-enter your password.</p>
--

How to Check in a Conference Leader style guest

Use these instructions if the you wish to issue 'Conference Leader' style keys to certain guests.

A guest with a Conference Leader style keycard will have normal access to their own room, and special access to one or more Conference or Meeting Rooms. When they use their keycard in these rooms, the door will remain unlocked – allowing easy entry for other delegates / attendees. At the end of the conference or meeting, the Conference Leader can again use their keycard – this time the door will lock.

Other valid keys will work in the lock as follows :

- If the door is unlocked, no effect.
- If the door is locked, normal operation – unlock then relock after approx 5 seconds (configurable).

Conference Leader style keycards must be Smart Cards – and therefore the Conference or Meeting Rooms in question must be capable of accepting Smart Cards. Check the Lock type Report if you are unsure.

The Conference or Meeting Rooms in question must have been set up in their own lock group (Setup module). This lock group must have been set as 'Custom Locks' and have the 'Stay Unlocked' option activated. The locks must then have been added to any guest keycard type that you will use when issuing 'Conference Leader' style keycards.

1. From the check in screen **Main** tab, fill out the normal required information. Guest (bed)room, start and end dates and times, User Type, Common Doors etc. *Remember, the User Group must be one that issues Smart Cards*
2. On the **Names** tab fill out the guest name (not compulsory).
3. Go to the **More Rooms** tab. In one of the More rooms boxes, enter the name of one of the conference / meeting room doors. An **Unlock** button will appear. Press it.
Repeat for up to 5 meeting / conference rooms.

If you leave the Unlock button unselected for one or more rooms, the guest keycard will simply have normal (as opposed to 'Stay Unlocked') access to that room.

You can allocate other normal (bed)rooms to the guest on the more rooms screen too. No unlock button will appear for these.

4. Press **Encode** to make the Smart Card

Checking out a Guest

About Checking out a Guest

Most hotels will probably not need to use this feature for a couple of reasons:

- when a newer guest keycard is used on a room, the previous guest's keycard will no longer unlock the door

- guest keycards automatically expire after the check out date and time that is encoded on the keycard

Your hotel however, may have reasons for wanting to determine if a guest has actually checked out or not. For example, some hotels, use Property System Management (PMS) software that checks to see if the guest has checked out before allowing charges (such as phone calls) to be made to the room. Unless you use the Check Out feature of the Vision system, you will not be able to verify whether they have actually checked out.

If you are unsure of whether or not your hotel uses this feature, check with your hotel's Vision system administrator.

<p>NOTE: Using the Check Out feature will not invalidate the guest's keycard, it will only indicate to the Vision system that the room is now vacant.</p>

How to Check out a Guest

Some hotels do not use this feature, see your Vision System Administrator if you are unsure of whether you need to Check Out guests.

1. If the Check In screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Guest Keycards**.
2. From the **Check In** screen, touch **Back** to go to the **Guest Keycards** menu screen.
3. Select the **Room** number from the list on the left of the screen. If the current guest keycard for the room is checked into connecting rooms, just enter any one of the room numbers.
4. Touch **Check Out** to display the Check Out screen.
5. If a list of cards is shown, select the card you want to check out (refer to dates, name tab etc). To check out the whole list, repeatedly press **Remove** then **Back** then **Check Out**.
6. To select a different **Room** number, use the keypad on the right of the screen. If the current guest keycard for the room is checked into connecting rooms, just enter any one of the room numbers.
Whenever you select a different room number, you will need to touch **Find** to update the screen with the new room number information.

NOTE: After a few minutes of inactivity, the Login screen will be displayed and you will need to re-enter your password.

Changing the Checkout Date or Time

About Changing the Check out Date or Time

Normally, you will use this to **extend** a guest's check out date or time. You will not normally need to use this for early check outs, because when a new guest uses their room keycard on the room, any older guest keycards will no longer open the lock.

Changing a check out date results in issuing a new guest keycard (you can of course recode the same physical card). After the new keycard is used on the room, their old keycard (and any existing Duplicate keycards) will no longer open the lock.

NOTE: If you use Change and there are any roommates, you will need to make new Duplicate keycards for them as well.

How to Change the Check out Date or Time

Change guest card

Encode Find Help Logout Back

Main Name More Rooms

Room
501,502

From date/time
07/10/2002 07:33

Until date/time
09/10/2002 07:35

User group
PAX CABIN

Common doors
Yes

7 8 9
4 5 6
1 2 3
0 BkSpc

© Copyright 2002 by VingCard 14:17:31 07/10/2002

Although you can use Change to change anything on a guest keycard, usually it is used to extend the check out date.

1. If the Check In screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Guest Keycards**.
2. From the **Check In** screen, touch **Back** to go to the **Guest Keycards** menu screen.
3. Select the **Room** number from the list on the left of the screen.

4. Touch **Change** and make any changes you need. Touch **Encode**.

NOTE: A new card will only be made if new information needs to be written to the card. For example, if you correct the spelling of a guests name, the information is saved in the Vision database but not written to the card – therefore no actual encoding will take place. When changing end date, a new card needs to be encoded.

Making Duplicate Keycards

About Duplicate Keycards

These keycards are normally made when additional keycards are needed for roommates. You can make several keycards at a time, by selecting the number of cards you want to make when checking in a guest. However, if you wish to tag an individual name to each card or if you want to make duplicates some time after the initial check in refer to the following step-by-step instructions.

NOTE: For security purposes, if a keycard is lost or stolen, you should always Replace the keycard rather than making a Duplicate.

How to Make a Duplicate Keycard

Use these instructions if you want to issue additional keycards for a guest who is already checked in.

1. If the Check In screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Guest Keycards**.
2. If the correct room number is not already selected on the **Room** tab, use the number pad on the right side of the screen to enter the Room Number.

If you are making a duplicate of a keycard which can open the lock of more than one room, touch the **More rooms** tab, and enter the numbers of the additional rooms the keycard should be able to open.

If you are making a duplicate for a suite, use the **Type** button to select the suite.

If you wish to add the guest name, use the **Names** tab

TIP: *Do NOT change the check in/out dates while making duplicates. The result would be that the original keycard would be valid in a different period than the duplicates. To change a guest's stay, use Change to make a new keycard and at the same time, make the duplicates.*

3. To change the number of **Cards** you want to make at this time, touch the displayed number, then select the correct number from the number pad on the right side of the screen. It is not necessary to change any other selections on the Check In screen.

TIP: *If you wish to tag unique guest names to each card made you should make one card at a time, enter the names for each cardholder on the **Names** tab and select 'Copy Old' after pressing the **Encode** button..*

4. Touch the **Encode** button when you are ready to make the duplicates.
5. A message will display indicating that there is a valid keycard for this room. Touch **Copy Old**.



You will be prompted to insert as many keycards into the encoder as you requested.

NOTE: After a few minutes of inactivity, the Login screen will be displayed and you will need to re-enter your password.

Replacing Lost or Stolen Keycards

About Replacing Lost or Stolen Keycards

Replacing keycards is normally done if a guest keycard is lost or stolen. After the new keycard is used to open the room, their old keycard will no longer open the lock. However, any existing Duplicate keycards (roommates) will still open the lock.

For security purposes, if a keycard is lost or stolen, you should always Replace the keycard rather than performing a new check in or making a Duplicate.

Whenever a new room keycard is made, the Vision system assigns a unique ID to it. This ID is used to identify keycards when interrogating locks. Replaced keycards retain this ID on the replacement keycard, so it is recommended that you use Replace rather than performing a new Check In to replace the keycard.

NOTE: If there are any roommates and you Replace a guest keycard, you will NOT need to make new Duplicate keycards for the roommates.

How to Replace a Lost or Stolen Keycard

For security purposes, you will need to Replace lost or stolen keycards, rather than duplicate them.

Replace guest card

Encode Find Help Logout Back

Main Name More rooms

Room
501,502

From date/time
07/10/2002 07:33

Until date/time
09/10/2002 07:35

User group
PAX CABIN

Common doors
Yes

7 8 9
4 5 6
1 2 3
0 BkSpc

© Copyright 2002 by VingCard 14:24:51 07/10/2002

1. If the Check In screen is not displayed, touch the **Back** button to return to the Vision **Main** menu.
2. Touch **Back** to display the **Guest Keycards** menu screen.
3. Select the **Room** number from the list on the left of the screen.
4. Touch **Replace** to display the Replace guest card screen.
5. Touch **Common door** if you want to view or change the common doors for this guest.
6. If you Replace a guest's keycard, you will **NOT** need to make new duplicates for any roommates.
7. Touch **Encode** to make the keycard.

Viewing the Information on a Guest Keycard

About Viewing the Information on a Guest Keycard

Using the View Keycards feature allows you to “read” guest keycard data stored in system database:

- Room number(s)

- Guest name
- PMS ID
- User Group
- Whether the guest has access to Common doors

You can use **System Events** in the **Reports** module to determine which employee made a guest keycard. Alternatively, if you have the card, you can **Verify** it and examine the '**More Data**' tab to find details of when the card was made, changed etc.

How to View the Information on a Guest Keycard

Displaying information about a guest keycard is helpful, when hotel personnel wants to check if there are any cards (valid or pre-checked) issued to given room.

View guest card

Room: 501,502

Keycard for: suite2

PMS ID:

User group: PAX CABIN

Common doors: Yes

Cards: 1

Cards found:

Name	Start date/time	End date/time
June Potter	07/10/2002 05:33:00	09/10/2002 07:35:00

© Copyright 2001, by VingCard

1. If the Check In screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Guest Keycards**.
2. From the **Check In** screen, touch **Back** to go to the **Guest Keycards** menu screen.
3. Select a room from list.
4. Touch **View**. If a list of cards is shown, it means there is more than one card issued for the room.

5. To view another room, enter the room number and touch **Find**.

Verifying the Information on a Guest Keycard

About Verifying the Information on a Guest Keycard

Using the Verify Keycards feature allows you to “read” a guest keycard and display the following information:

- Room number(s)
- Check In date/time
- Check Out date/time
- User Group
- Whether the guest has access to Common doors
- Issue area
- Extended Card History (via the **More Data** tab)

NOTE: If you attempt to use the Guest Keycards module to Verify a blank keycard, a damaged keycard, a keycard made from a different module, or a keycard from a different hotel, an error message will be displayed.

How to Verify the Information on a Guest Keycard

Displaying information about a guest keycard is helpful if a guest forgets his room number or a keycard is found.

Verify guest card

Verify Help Logout Back

Main Name More rooms Result More Data

Room
501

From date/time
07/10/2002 12:46

Until date/time
17/10/2002 12:00

User group
PAX CABIN

Common doors
Yes

Keycard for
PAX CABIN

Issue area
1

Result
Valid keycard.

© Copyright 2002 by VingCard 14:47:17 07/10/2002

1. If the Check In screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Guest Keycards**.
2. From the **Check In** screen, touch **Back** to go to the **Guest Keycards** menu screen.
3. Touch **Verify**. You will be prompted to insert a keycard into the card reader.
TIP: *For security purposes, the Card Encoder is set to wait for a brief period and if a keycard is not inserted, the process will be cancelled.*
4. Examine the card information. To view extended card history information, go to the More Data tab. You will find a time ordered list of all the operations (for example Check In, Change, Replace) carried out on this card. If you double click on an item on the list, you will find further detail about the operation : which staff member carried on the operation, on which PC etc.

Result		More Data
Event time		Description
07/10/2002 14:46		Check in new guest, remove pi
07/10/2002 14:46		Change guest information
		Employee: VingCard, Demo1
		Employee id: VingCard 1
		Station: DEV08ED
		StartTime: 07/10/2002 12:46
		EndTime: 17/10/2002 12:00
		Keycard options: Multiple rooms
07/10/2002 14:46		Verify guest keycard
07/10/2002 14:58		Verify guest keycard
Change guest information		

5. To read another guest keycard, touch **Verify** and insert the next keycard.

NOTE: If you attempt to use the Guest Keycards module to Verify a blank keycard, a keycard made from a different module, or a keycard from a different hotel, an error message will be displayed.

Employee Keycards Module





What the Employee Keycards Module Does

The Employee Keycards module allows you to make keycards for specific employees.

Use the Employee Keycard module to do any of the following:

- Add a new employee keycard (such as for Maids, etc.)
- Change employee information (name, employee ID, or User Group)
- Replace a lost, stolen, or expiring employee keycard
- Replace a damaged employee keycard
- Remove employee information from the Employee Keycards module
- Verify the information for any employee keycard

NOTE: The Employee Keycards and System Users modules share the same employee information. Therefore using Add or Change from either, will automatically update the other.

Quick Steps to Using the Employee Keycards Module

This topic was designed as a quick reference. For more details on each task, touch the **Help** button and select the appropriate Help topic.

Task	Beginning from the Employee Keycards screen:
Adding a New employee to the Employee Keycards module	<ul style="list-style-type: none"> Press Add (New tab is selected) Press the keyboard button for Employee Id. and enter the information Press Enter on the keyboard to return to the Add employee screen Repeat steps 2 and 3 for Last name and First name Press User group and select one Press Save Insert the keycard for encoding
Adding an employee from the System Users module	<ul style="list-style-type: none"> Press Add Press System user tab Select the name of the employee from the list on the right side of the screen Press User group and select a User Group Press Save Insert the keycard for encoding
Changing Employee Information	<ul style="list-style-type: none"> Select the name of the employee you want to make Changes to Press Change Press the keyboard button for the items you want to change and enter the information Press Save If you changed the User Group, insert a keycard for encoding
Replacing a damaged Employee Keycard	<ul style="list-style-type: none"> Press the name of the employee you want to make the new keycard for Press Change Press Save without making any changes to the screen Insert the keycard for encoding
Replacing a single lost or stolen Employee Keycard	<ul style="list-style-type: none"> Select the name of the employee Press Replace Select 'Replace this keycard and cancel old' Press OK to continue Insert a keycard Press OK to continue
Replacing all Employee keycards in a User Group (because the expiry date is approaching)	<ul style="list-style-type: none"> Click the Usergroup column header to group all employees by User Group. Select the name of one employee in the relevant User Group Press Replace Select 'Replace all keycards in user group' Press OK to continue Insert a keycard Press OK to continue Repeat for keycards for all other User Group members
Removing an employee from the Vision system	<ul style="list-style-type: none"> If the employee is on a Void-list, remove them from it Select the name of the employee you want to Remove Press Remove Press Yes

Using Verify to display the information on an Employee Keycard	<ul style="list-style-type: none"> • Press Verify • Insert the employee keycard

Comparison of Keycards Made from Employee Rooms Module

Both the **Employee Keycards** module and the **Employee Rooms** module make keycards for use by employees. However, they each serve different purposes:

Module	Making the Keycard	What it does	Examples
Employee Keycards	Keycards are made by selecting a specific employee (by name). The keycard will normally be valid for up to 2 years.	The keycard will unlock all doors for the User Group this employee belongs to. No additional access can be assigned when the keycard is made.	Make keycards for maids Make keycards for bellhops
Employee Rooms	Keycards are made by selecting an Employee Type (such as Repairman) instead of employee name. (You may also enter the employee name in this module.) The keycard can be made to expire after one use, or have an expiration date specified when making the keycard.	The keycard will unlock the room number you selected when making the keycard. When making the keycard, you can also select from the Common Doors list for additional access. These keycards can be made for outside vendors as well as employees.	Make a One-shot keycard to allow delivery of flowers to a banquet room Make a keycard that will allow a repairman to enter a room for one week Check employees into cabins on a cruise ship

Adding an Employee to the Employee Keycards Module

About Making a New Employee Keycard

Before you can make an employee a keycard, you must Add the employee to the Employee Keycards module. To do this you can either enter New information or select employee information that was entered in the System Users module.

For security purposes, employee keycards are made for each individual employee. The keycard includes the Employee ID, employee name, and User Group.

The User Group you choose when making an employee keycard determines the following:

- Which doors the keycard will open
- The expiration date of the keycard
- The Keycard Type

- Times of the day the keycard can be used
- Deadbolt override access

Unlike making Employee Rooms keycards, you cannot select Common Doors for additional access when making the keycard – their access is determined **solely** by User Group.

The length of time employee keycards will be valid, is 2 years from the date they were created.

NOTE: The Employee Keycards and System Users modules share the same employee information. Therefore using Add or Change from either, automatically update the other.

Adding an Employee from the System User Module

Add employee		Save	Help	Logout	Back						
<div> <div>New System user</div> <div> <div> <div>Employee Id.</div> <input type="text"/> </div> <div> <div>Last name</div> <input type="text"/> </div> <div> <div>First name</div> <input type="text"/> </div> <div> <div>User group</div> <input type="text"/> </div> </div> <div> <table border="1"> <thead> <tr> <th>Name</th> <th>Id</th> </tr> </thead> <tbody> <tr> <td>Mellie, Roger</td> <td>f100</td> </tr> <tr> <td>VingCard, Demo2</td> <td>VingCard 2</td> </tr> </tbody> </table> <div> <div>⬆</div> <div>⬆</div> <div>⬆</div> <div>⬆</div> <div>⬆</div> <div>⬆</div> </div> </div> </div>						Name	Id	Mellie, Roger	f100	VingCard, Demo2	VingCard 2
Name	Id										
Mellie, Roger	f100										
VingCard, Demo2	VingCard 2										

© Copyright 2002 by VingCard

10:48:36 | 08/10/2002

1. If the main Employee Keycards screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Employee Keycards**.
2. Touch **Add** to display the **Add** employee screen.
3. Touch the **System user** tab to display the list of employees to select from.
4. Touch the name of the employee you want to make the keycard for. All of the information on the left side of the screen will be filled in for you, except the User Group.
5. Touch the **User group** window and select a User group from the list that

appears on the right of the screen.

6. Touch the **Save** button and you will be prompted to insert the keycard for encoding.
7. After the keycard is encoded, you will be returned to the **Employee Keycards** menu screen.

Adding an Employee that is New to the Vision System

1. If the main Employee Keycards screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Employee Keycards**.
2. Touch **Add** to display the Add employee screen. The **New** tab will already be selected.
3. Touch the **Keyboard button** that appears after the Employee Id. Window.
TIP: *For more information on using the Keyboard, refer to the How to Use the On-screen Keyboard illustration following these instructions.*
4. After entering the employee's ID number, press **Enter** to return to the Add Employee screen.
TIP: *For Employee ID., you can enter any alphanumeric ID number you wish, as long it is unique to this employee. This same Employee Id number will be used in the System Users module, if you give this employee System Access.*
5. Use the keyboard buttons after the **Last Name** and **First Name** as you did for Employee ID. to enter the information for both of them.

6. Touch the **User group** window and select a User group from the list that appears on the right of the screen.
7. Touch the **Save** button and you will be prompted to insert the keycard for encoding.
TIP: *The Employee Keycards and System Users modules share the same employee list. Therefore, you only have to use **Add New** to enter the employee information once and then can select it from the other module.*
8. After the keycard is encoded, you will be returned to the **Employee Keycards** menu screen.

Replacing Employee Keycards

Determining What Method to Use to Replace an Employee Keycard

Read this to help you determine whether to use Replace, Change, or to Remove the employee keycard and make a new one:

- If the employee keycard is damaged, use the **Change** option to make a new one exactly like the damaged one. The old employee keycard will not be invalidated by the new keycard, so use this only after you destroy the old employee keycard. The old expiration date is unaffected.
- If the employee keycard is lost or stolen, use **Replace : Replace this keycard and cancel old** to prevent the lost employee keycard from opening doors. Using the new replacement card in all locks accessible by employee, will invalidate the old (lost) keycard without causing you to remake the keycards for any other employees.
- Employee keycards normally expire after 2 years. Use the **Replace : Replace all keycards in user group** option to make new keycards for all members of a user group.

Replacing Lost, Stolen, or Expiring Employee Keycards

About Replacing Expiring Employee Keycards

Employee keycards expire after two years. You will need to use the **Replace : Replace all keycards in user group** option when employee's keycards are about to expire.



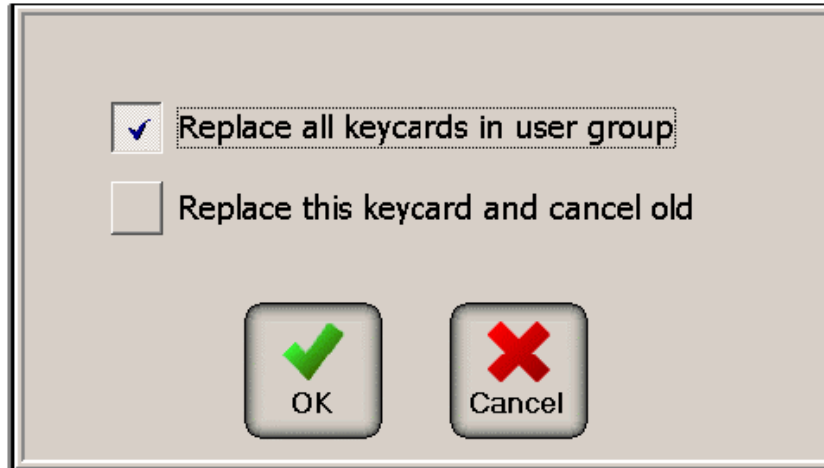
WARNING! If you do a **Replace : Replace all keycards in user group** for one user group you may need to replace the employee keycards for other user groups too – if there are other user groups that share the same keycard type (for example user groups 'Maid Floor 2' and 'Maid Floors 2 and 3' could both be of underlying keycard type 'Maid'). To make this process easier for you, the Vision system will check to see which User Groups you need to Replace keycards for and will display a message listing all User Groups that will be affected.

You need to Replace the keycards for ALL employees in ALL of the User Groups that are listed, even if their keycards are not expired.

How to Replace an Expired Employee Keycard

If you **Replace** an employee's keycard, you will need to Replace the employee keycards for all User Groups with the same Keycard Type.

1. If the main Employee Keycards screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Employee Keycards**.
2. Click on the 'Usergroup' column heading to sort the employees according to user group, then select the name of one of the employees you want to make new keycard for.
3. Press **Replace** and select **Replace all keycards in user group**



4. A message will appear listing all of the User Groups that you will also need to Replace keycards for.



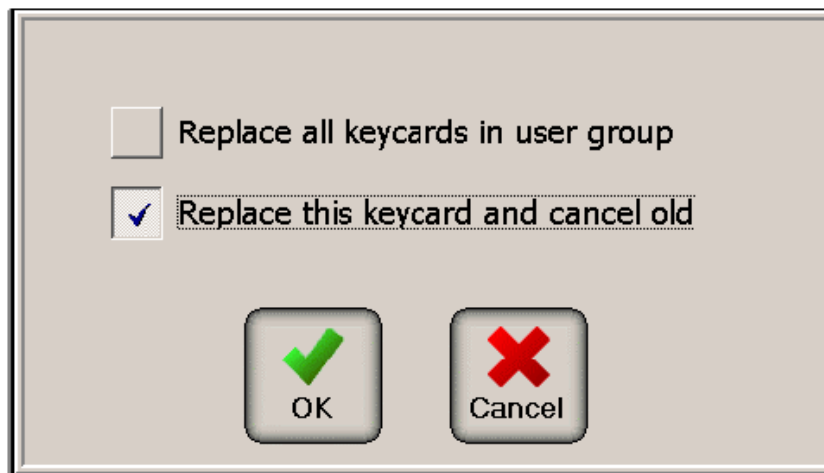
5. Press **Yes** and you will be prompted to insert a keycard for encoding. You can insert any keycard. A new expiration date (2 years in the future) will automatically be assigned to the keycard.
6. After the new keycard is made, you will see a message indicating that the card was successfully replaced. Touch **OK** and you will be back to the **Employee Keycards** menu screen.
7. Select the next affected employee from the list and select replace. Insert the keycard when prompted.
8. Repeat step 6 for all affected employees.
9. Once any of the new employee keycards is used in an individual lock, none of

the old keycards will open the lock.

How to Replace a Lost or Stolen Employee Keycard

You can **Replace** an individual employee's keycard without the need to replace any other employee keycards.

1. If the main Employee Keycards screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Employee Keycards**.
2. Click on the 'Usergroup' column heading to sort the employees according to user group, then select the name of one of the employees you want to make new keycard for.
3. Press **Replace** and select **Replace this keycard and cancel old**.



4. Touch **OK** and you will be prompted to insert a keycard for encoding
5. After the new keycard is made, you will see a message indicating that the card was successfully replaced. Touch **OK** and you will be back to the **Employee Keycards** menu screen.
6. The new keycard contains information about the old (lost) card. Once the new keycard is used in an individual lock, the lock reads this information and ensures that the old (lost) keycard will not open the lock. To ensure that the old (lost) keycard is not used, you should use the new keycard in ALL locks that the employee has access to.

NOTE : All other employee cards will continue to work as normal.

Using Change to Replace a Damaged Employee Keycard

About Replacing Damaged Employee Keycards

Use the Change option, not the Replace option to replace damaged keycards or to make duplicates of an employee keycard.

Whenever you use the **Change** option and touch Save without making any changes to the employee information, you will be asked to insert a new keycard for encoding. The result is a new employee keycard exactly the same as the old keycard, including the expiration date.

NOTE: Even if the old keycard does not seem to work in any locks, it is possible that the fault tolerance will vary slightly between locks. For security purposes, you should destroy it before using the Change option to make a new one.

No other employee's keycard is affected by making keycards with the Change option.

How to Use Change to Replace a Damaged Employee Keycard

1. If the main Employee Keycards screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Employee Keycards**.
2. Touch the name of the employee you want to make a new keycard for.
3. Touch **Change** to display the Change employee screen. Do not make any changes.
4. Touch the **Save** button and insert a keycard for encoding.
TIP: *An existing employee keycard that is damaged should be destroyed as it may still open some locks.*
5. After the keycard is encoded, you will be returned to the **Employee Keycards** menu screen.

Changing Employee Information

About Changing Employee Information

You can change Employee information such as employee ID or name.

You can also change user group, thus giving the employee access to a different set of doors. **This will not involve changing any other cards or reprogramming any doors.**

- When you use Change, the expiration date of the employee keycard is unaffected.
- Change does not affect any other employee's keycards.
- The old keycard is not invalidated by the new keycard and even a damaged keycard may still open some locks. So, for security purposes, you should destroy the old keycard (or recode the existing card).

NOTE: If this employee has System Access, the changes you make in the Employee Keycards module will automatically update the employee information in the System User module.

How to Change Employee Information

Change employee

Save Help Logout Back

Change

Employee Id.
m102

Last name
Troy

First name
Helen

User group
Maid night 3/4

User groups

Banquet dept
Emergency
Housekeeper
Maid day 1st Fl
Maid day 2nd fl
Maid day 3rd fl
Maid day 4th fl
Maid night 1/2
Maid night 3/4
Maintenance
Master

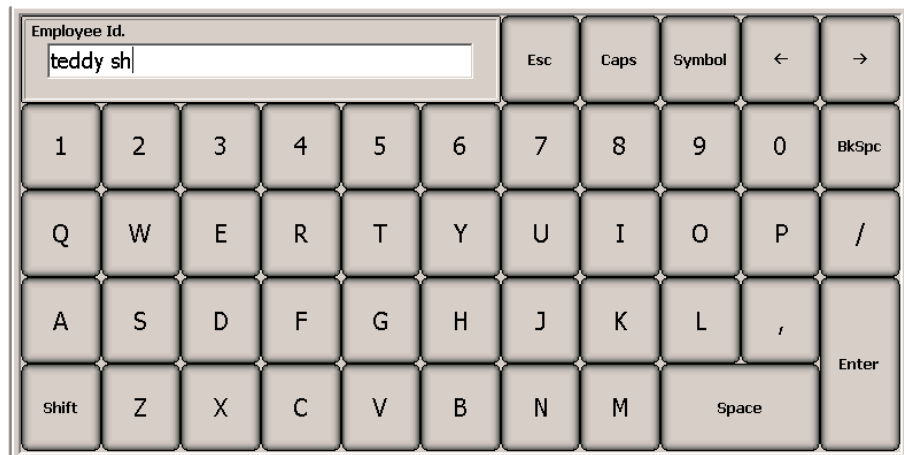
© Copyright 2002 by VingCard 10:49:37 08/10/2002

1. If the main Employee Keycards screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Employee Keycards**.
2. Touch the name of the employee you want to Change information for.
3. Touch **Change** to display the Change Employee screen.

4. Touch the **Keyboard button** that appears after the item you want to change (Employee Id., Last name, or First name).
TIP: *For more information on using the Keyboard, refer to the How to Use the On-screen Keyboard illustration following these instructions.*
5. If you want to change the **User Group**, touch the User group window and select from the list that appears on the right of the screen.
6. When you have finished with this screen, touch **Save**. You will only be prompted to insert a new keycard for encoding if you changed the User Group (makes a keycard that matches this new User Group) or changed nothing on the screen (makes a duplicate replacement keycard).
7. After the keycard is encoded, you will be returned to the **Employee Keycards** menu screen.

NOTE: If this employee has been added to the System Users module, it will be updated by any changes you make to name or employee ID.

How to Use the on screen keyboard



Esc = Cancel

Caps = capitalize continuously

Symbol = show symbol keyboard

Arrow buttons = move cursor

BkSpc = erase one character at a time

Shift = capitalize one character

When you have finished with the keyboard, press enter

Removing an Employee from the Vision System

About Removing an Employee from the Employee Keycards Module

Removing an employee does NOT invalidate their keycard. Also, using Remove does not affect any other employee's keycard.

You should use remove when an employee stops working at a property **and has turned in their keycard (confirmed by the verify function).**

If a leaving employee does not hand in their keycard when quitting, you can invalidate their card either by :

- Doing a **Replace this keycard and cancel old** operation for the employee, then using the replacement card in all locks where the employee had access, then destroying the new (replacement card) then removing the employee

OR

- Adding the employee to the void list, making a void list card, then using the void list card in all locks where the employee had access. See Special Cards module for help on void list. *The advantage of void list cards is that many employees can be denied access to locks in one go.*



WARNING!

Read the following information before using Remove.

- Employees cannot be taken off of the Void-list after they have been Removed. You need to take them off of the Void-list prior to using Remove.
- After using Remove, you can no longer use Verify to view the information on their employee keycard. Therefore, it is not recommended that you use Remove unless you have first used Verify to determine that the correct employee keycard has been turned in. If they do not turn in their employee keycard, or if the employee keycard was damaged and cannot be read, it is not recommended that you Remove them.
- After using Remove, if you interrogate a lock to determine what keycards were used on it, the User Group and Keycard Type will be shown but the employee name is not guaranteed to be shown. *The old employee information will be retained for a period of time.*
$$=(4000\text{-total staff}) / (\text{average daily staff turnover}) \text{ days.}$$
The higher the turnover in employees, the lower the retention time. So, even a property with a staff of 2000 and a turnover of 20 employees a day would retain the information for 100 days.

How to Remove an Employee from the Vision System

NOTE: If this employee has System Access, they will also be removed from the System Users module.

1. If the employee is on a Void-list, remove them from it. See the Special Keycards module Help for instructions.
2. If the main Employee Keycards screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Employee Keycards**.
3. Touch the name of the employee you want to Remove.
4. Touch **Remove**.
5. A message will appear asking you to confirm the deletion. Touch **Yes**. This process removes the employee from the Employee Keycards module, but does not invalidate the employee's keycard.



6. You will be returned to the **Employee Keycards** menu screen.

Viewing Employee Information

Displaying the Information on an Employee Keycard

About Displaying the Information on an Employee Keycard (Verifying)

If you have possession of an employee keycard, you can use Verify to view the following information about the keycard:

- Employee ID
- Name
- User Group
- Date the keycard was issued
- Expiration date
- Whether the keycard is currently valid
- Extended Card History (via the **More Data** button)



For security reasons, the Employee's password is not included in this information.

If you do not have the employee keycard in your possession, you can display this same information by selecting the employee's name and touching Change.

NOTE: If you attempt to use the Employee Keycards module to Verify a blank keycard, a keycard made from a different module, or a keycard from a different hotel, an error message will be displayed.

How to Display Information on an Employee Keycard

Verify employee

Data

Employee Id.
m102

Last name
Troy

First name
Helen

User group
Maid night 1/2

Keycard valid from
Date: 06/08/2002
Time: 11:25:55

Keycard valid to
Date: 05/08/2004
Time: 11:25:55

Result
Valid employee keycard.

© Copyright 2002 by VingCard 10:52:26 08/10/2002

1. If the main Employee Keycards screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Employee Keycards**.
2. Touch **Verify**. You will be prompted to insert the employee keycard. Select either mag strip or Smart Card as appropriate.
3. Examine the card information. To view extended card history information, use the More Data button.

You will find a time ordered list of all the operations (for example Check In, Change, Replace) carried out on this card. If you double click on an item on the list, you will find further detail about the operation : which staff member carried on the operation, on which PC etc.

Verify employee

Verify

Help

Logout

Back

Data

Employee Id.

m102

Last name

Troy

First name

Helen

User group

Maid night 1/2

Event time	Description
08/10/2002 10:47	Add employee keycard Employee: VingCard, Demo1 Employee id: VingCard 1 Station: DEV08ED StartTime: 06/08/2002 11:25 EndTime: 05/08/2004 11:25
08/10/2002 10:52	Verify employee keycard

Add employee keycard

© Copyright 2002 by VingCard

10:53:05 08/10/2002

4. Touch the **Back** button to return to the Employee Keycards screen.

NOTE: If you attempt to use the Employee Keycards module to Verify a blank keycard, a keycard made from a different module, or a keycard from a different hotel, an error message will be displayed.

Displaying Employee Information Without Using a Keycard

About Displaying Employee Information Without Using a Keycard

By selecting the employee from the list and touching Change, you can view the following information:

- Employee ID
- Name
- User Group
- Whether an employee has access to any Vision modules

NOTE: To print a list of all employees, refer to the Reports module.
--

For security reasons, the Employee's password is displayed only when it is originally assigned, and not in any other report or screen.

If an employee has been issued a keycard and you have it in your possession, you can use **Verify** to view the information, including Extended Card History information.

How to Display Employee Information Without Using a Keycard

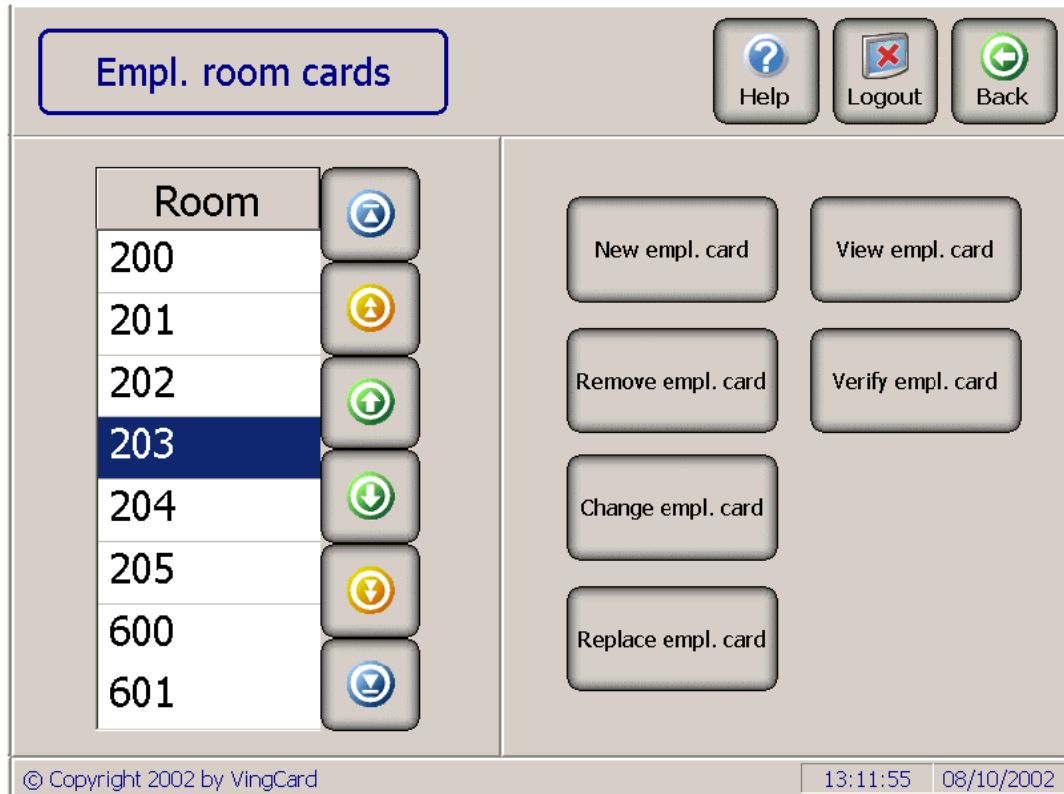
1. If the main Employee Keycards screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Employee Keycards**. All employee keycard holders' names and Employee Id's will be listed.

TIP: *If you want to know if this employee is a Vision system user and which specific modules this employee has access to, see the **System Users** module.*

*You can use the **Reports** module to print a report on the employee information.*

Employee Rooms Module





What the Employee Rooms Module Does

The Employee Rooms module will normally be used to give an employee or vendor access to a specific room. For example, to allow a repairman or a bellboy access to a guest room.

This module can also be used to check employees into a room or cruise ship cabin.

Like guest keycards, the Employee Rooms keycards may include access to other Common Doors.

You can use the Employee Rooms module to perform any of these tasks:



- Check in an employee into and out of one or more rooms (for example, cabins on a cruise ship)
- Make a keycard for an employee or vendor, that opens a specific door (for example, for a repairman)
- Change the keycard made with this module (for example, to extend the expiration date)
- Make duplicates of Employee Rooms keycards


- Replace lost or stolen Employee Rooms keycards
- View the information on a keycard that was made from this module
- Verify (read) the information on a keycard that was made from this module

NOTE: Using an Employee Rooms keycard will invalidate any older Employee Rooms keycards for the room. However, it will not invalidate guest room keycards.

Quick Guide to Using Employee Rooms Module

This Help topic was designed as a quick reference. For more details on each task, touch the **Help** button and select the appropriate Help topic.

Task	Beginning from the New Empl. Card screen:
Make Employee Rooms keycard	<ul style="list-style-type: none"> • Enter Room Number • If you have more than one Employee Rooms Keycard type defined (by setup) touch the  Keycard Type button and select the correct option. (Example : you might have a Repair Worker keycard type and a Flower Delivery Keycard type who may both be issued keycards to access a defined guest room). • Touch the Name tab and enter employee name. • Touch the More rooms tab and enter room numbers, if making a keycard valid for more than one room • Select check in/out dates and times. • Change Common Door options if required • Select Name tab and enter employee name if required • Touch the More rooms tab and enter room numbers, if making a keycard valid for more than one room • Touch Encode • Choose Make new if a popup appears indicating room is occupied
Duplicate Employee Rooms keycards	<ul style="list-style-type: none"> • Enter Room Number (and appropriate 'more rooms' numbers) • Use the Keycard Type button  to select the correct keycard type. • Select Name tab and enter new name if required • Touch Encode • Select Copy Old from popup
Replace Employee Rooms keycard	<ul style="list-style-type: none"> • Touch Back • Choose a Room number • Touch Replace empl. Card • If a list of cards is shown, select the card you want to replace (refer to dates, name tab etc) • Touch Encode
Remove Employee Rooms keycard from the Vision system	<ul style="list-style-type: none"> • Touch Back • Choose a Room number • Touch Remove empl. Card • If a list of cards is shown, select the card you want to replace (refer to dates, name tab etc) • Touch Remove

One-shot Keycards	<ul style="list-style-type: none"> • Enter Room Number • Touch the Keycard Type button  and select "One shot" (or whatever your hotel named it) • Select Name tab and enter name if required • Touch Encode • Choose Make new if popup appears indicating room is occupied (i.e. a non time expired one-shot card is already issued)
View Employee Rooms Keycard	<ul style="list-style-type: none"> • Touch Back • Choose a Room number • Touch View empl. card • Enter room number and touch Find to view other rooms
Verify Employee Rooms Keycard	<ul style="list-style-type: none"> • Touch Back • Touch Verify empl. card • Insert keycard when prompted • Touch Verify to verify additional keycards

Comparison of Keycards made from Employee Keycards Module

Both the **Employee Keycards** module and the **Employee Rooms** module make keycards for use by employees. However, they each serve different purposes:

Module	Making the Keycard	What it does	Examples
Employee Keycards	Keycards are made by selecting a specific employee (by name). The keycard will normally be valid for up to 2 years.	The keycard will unlock all doors for the User Group this employee belongs to. No additional access can be assigned when the keycard is made.	Make keycards for maids Make keycards for bellhops
Employee Rooms	Keycards are made by selecting a Keycard Type (such as Repairman or One-shot) instead of employee name. (You may also enter the employee name in this module.) The keycard can be made to expire after one use, or have an expiration date specified when making the keycard.	The keycard will unlock the room or rooms you selected when making the keycard. When making the keycard, you can also select from the Common Doors list for additional access. These keycards can be made for outside vendors as well as employees.	Make a One-shot keycard to allow delivery of flowers to a banquet room Make a keycard that will allow a repairman to enter one or more rooms for one week Check employees into cabins on a cruise ship

Making an Employee Rooms Keycard

About Making Employee Rooms Keycards

The Vision system allows each hotel to customize the encoding of keycards to meet their needs. Therefore, some of these options will vary depending on the decisions your hotel made:

- **User Groups** – Whenever you make an Employee Rooms keycard, you must specify a User Group. Different User Groups have different access. For example, your hotel may have a User Group with access to a VIP floor.
- **Keycard Type** – In addition to User Groups, your hotel also sets up an Keycard Type list, such as “One-shot” keycards or “Repairman”. In addition to selecting a User Group, you must **always** make a selection from the Keycard Type list whenever you make an Employee Rooms keycard. This list is displayed from the button on the right of the room number.
- **Common Doors** – In addition to access controlled by User Group and Keycard Type, you can optionally give an employee access to additional doors and locks, or give the employee Deadbolt Override access. These additional options are set up by your hotel. This list is displayed from the **Common Doors** button and is same list that appears when making Guest Keycards.

NOTE: If you are unsure of how your hotel uses any of these options, check with your hotel’s Vision system administrator.

How to Make an Employee Rooms Keycard

Use these instructions to check in an employee or make any other type of Employee Rooms keycard.

1. If the **New Empl. Card** screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Employee Rooms**.
2. Use the number pad on the right side of the screen to enter a **Room** number. If the keycard should be valid for more rooms, touch the **More rooms** tab, and enter up to two additional room numbers. If you want to enter the employee name on the card, touch the **Name** tab, and enter the first and last name of the employee.

TIP: *A to Z characters in room numbers – The number pad does not include alpha characters, so if your hotel has room numbers such as S201, be sure to select the room number from the main Empl. Room Cards screen before touching the **New empl. Card** button.*

*Checking Employees into Occupied rooms – Most hotels will want to be able to assign Guest Keycards and Employee Rooms Keycards to the same room so that repairs, etc. will not interfere with guest access. However, if you use the **Employee Rooms module to check employees into rooms**, check that the room is not already assigned to a guest.*

3. Touch the **Keycard Type** button (to the right of the room number) and select from the list. Each hotel creates their own Keycard Type list. If you are unsure of what these represent, see your hotel's Vision system administrator.

TIP: *Each hotel sets up their own Keycard Type list, such as “One-shot” keycards or “Repairman”. You must select from this list whenever you make an Employee Rooms keycard – unless you only have one type of Employee Rooms keycard defined.*
If you are unsure of what the selections in this list represent, see your hotel’s Vision system administrator.

4. To change the **From/Until Dates**, touch the displayed dates and then touch the correct date that appears on the right side of the screen.
5. To change the **From/Until Times**, touch the displayed times and then touch the position on the clock of the time you want to select.

If the AM and PM buttons appear under the clock, you can touch either of them to switch between AM and PM.

OR

If the 1-12 and 13-24 buttons appear under the clock, you can touch either of them to switch between the first and last 12 hours of the day.

TIP: *To determine whether to display a 12 or 24 hour clock, the Vision system will check to see which Regional Setting your hotel chose from the System Setup module. The two buttons under the clock will either be AM and PM (12:00 PM = Noon) or the first 12 or last 12 hours of the day (24 hour clock).*

6. To select a **User Group**, touch the displayed User Group and then select the correct User Group from the list that appears on the right.
7. If no **Common doors** are currently selected, a “No” will appear for this item. To view the list of selected doors, touch the displayed common doors Yes / No box. Touch any items on the list that appears on the right to select or deselect them.

As well as determining which common doors the guest can open, the list determines whether the keycard will have deadbolt override capability.



TIP: The User Group may have included default access to one or more of the Common Doors. However, you can add or remove access to any items on the Common Doors list.

Making selections from the list:

A red check mark to the left of the list indicates that access will be included with the keycard. Touching items on the list will select or deselect them.

8. To make more than one keycard (Duplicates), touch the displayed **Cards** selection and that appears on the right.

TIP: There is a second method of making duplicate keycards. This is useful if you need an additional Employee Rooms keycard for the room or if you want to add individual employee names for each card. See the “How to Make Duplicates of Employee Rooms Keycards” topic for more information.

9. When you have finished making all changes, touch the **Encode** button to make the keycard.

TIP: For security purposes, the Card Encoder is set to wait for a brief period and if a keycard is not inserted, the process will be cancelled.

When the new employee uses their keycard on the room, the previous room keycard will no longer open the room door.

10. When you make a new Employee Rooms keycard, the Vision system checks to see if there are any un-expired Employee Rooms keycards for the room. If there are, you will see a message indicating the room is still occupied. Touch **Make New**. You will be prompted to insert the number of keycards required.

Making a One-shot Keycard

About One Shot Keycards

Your hotel may have set up the Vision system to allow you to make a keycard that can be used only one time to open a lock.

One-Shot keycards allow access to a room for things such as flower delivery.

You could also make one for a guest if they accidentally locked their guest keycard in their room. This would allow them to retrieve their room keycard without invalidating it.



WARNING! If the Escape/Return key type option is selected (see Setup Module) a one shot card can only open a door, but not re-lock it.

NOTE: If you are unsure of which User Group or Keycard Type to select when making a One-shot keycard, check with your hotel's Vision system administrator.

How to Make a One-shot Keycard

The only difference between making a One-shot keycard and any other Employee Rooms keycard, is that you need to select the **User Group** and **Keycard Type** item that your hotel set up for this.

If you are unsure of which to select, check with your hotel's Vision system administrator.

Making Duplicate Employee Rooms Keycards

About Duplicate Keycards

You can make several keycards at a time, by selecting the number of cards to make whenever you make a keycard. However, this will not enable you to allocate a separate name to each keycard.

You can also make duplicates after encoding the first keycard. This way you can add duplicate cards at a later time (compared with the original card issue) or allocate individual names to all cards. See the step-by-step instructions for details.

In a situation where there is already a valid Employee Rooms keycard for a room and you need to give an additional employee a keycard, you can make a Duplicate.

Duplicate keycards differ from Replaced keycards and New keycards, in that they do not disable any existing Employee Rooms keycards for the room.

NOTE: For security purposes, if a keycard is lost or stolen, you should always Replace the keycard rather than making a Duplicate.

How to Make Duplicates of Employee Rooms Keycards

Use these instructions if you want to issue additional Employee Rooms keycards for a room.

1. If the **New Empl. Card** screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Employee Rooms**.
2. Use the number pad on the right side of the screen to enter a **Room** number. If the keycard should be valid for more rooms, touch the **More rooms** tab, and enter up to two additional room numbers (four for Smart Cards). If you want to enter the employee name on the card, touch the **Name** tab, and enter the first and last name of the employee.

TIP: ***A to Z characters in room numbers** – The number pad does not include alpha characters, so if your hotel has room numbers such as S201, be sure to select the room number from the main Empl. Room Cards screen before touching the **New empl. Card** button.*

***Checking Employees into Occupied rooms** – Most hotels will want to be able to assign Guest Keycards and Employee Rooms Keycards to the same room so that repairs, etc. will not interfere with guest access. However, **if you use the Employee Rooms module to check employees into rooms**, check that the room is not already assigned to a guest.*

3. To change the number of **Cards** you want to make at this time, touch the displayed number, then select the correct number from the number pad on the right side of the screen.

It is not necessary to change any other selections on this screen.

TIP: *If you wish to tag unique names to each card made you should make one card at a time, enter the names for each cardholder on the **Names** tab and select 'Copy Old' after pressing the **Encode** button..*

4. Touch the **Encode** button when you are ready to make the duplicates.

TIP: *For security purposes, the Card Encoder is set to wait for a brief period and if a keycard is not inserted, the process will be cancelled.*

When the new employee uses their keycard on the room, the previous room keycard will no longer open the room door.

5. A message will display indicating that there is a valid keycard for this room. Touch **Copy Old**.

You will be prompted to insert as many keycards as you requested.

NOTE: After a few minutes of inactivity, the Login screen will be displayed and you will need to re-enter your password.

Replacing a Lost or Stolen Employee Rooms Keycards

About Replacing Lost or Stolen Keycards

Replacing keycards is normally done if a keycard is lost or stolen. After the new keycard is used to open the room, their old keycard will no longer open the lock. However, any existing Duplicate keycards (roommates) will still open the lock.

For security purposes, if a keycard is lost or stolen, you should always Replace the keycard rather than performing a new check in or making a Duplicate.

Whenever a new room keycard is made, the Vision system assigns a unique ID to it. This ID is used to identify keycards when interrogating locks. Replaced keycards retain this ID on the replacement keycard, so it is recommended that you use Replace rather than performing a new Check In to replace the keycard.

<p>NOTE: If there are any roommates and you Replace a guest keycard, you will NOT need to make new Duplicate keycards for the roommates.</p>
--

How to Replace a Lost or Stolen keycard

For security purposes, you need to Replace lost or stolen keycards, rather than making Duplicates of them.

The screenshot shows the 'Replace empl. card' interface. At the top, there are five buttons: Encode, Find, Help, Logout, and Back. Below these is a sidebar with three tabs: Main, Name, and More rooms. The 'Main' tab is selected, displaying several input fields: 'Room' with the value '201', 'From date/time' with '08/10/2002' and '12:52', 'Until date/time' with '10/10/2002' and '14:00', 'User group' with 'Employee room', and 'Common doors' with 'No'. To the right of these fields is a large numeric keypad with buttons for digits 0-9 and a 'BkSpc' button. The bottom of the screen features a footer with the text '© Copyright 2002 by VingCard' on the left and a timestamp '13:53:38 08/10/2002' on the right.

1. If the New Empl. Card screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Employee Rooms**.
2. Touch **Back** to display the **Empl. Room Cards** menu screen.
3. Select the **Room** number from the list on the left of the screen.
4. Touch **Replace Empl. Card** to display the **Replace Empl. Card** screen.
5. If you Replace an employee's room keycard, you will **NOT** need to remake any duplicates.
6. Touch **Encode** to make the keycard.

Changing an Employee Rooms Keycard

About Changing an Employee Rooms Keycard

Normally, you will use this to **extend** an employee rooms card's expiry out date or time.

Changing a check out date results in issuing a new keycard (you can of course recode the same physical card). After the new keycard is used on the room, their old keycard (and any existing Duplicate keycards) will no longer open the lock.

NOTE: If you use Change and there are any roommates, you will need to make new Duplicate keycards for them as well.

How to Change an Employee Rooms Keycard

Change empl. card

Main Name More Rooms

Room
201

From date/time
08/10/2002 12:52

Until date/time
10/10/2002 14:00

User group
Employee room

Common doors
No

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

October 2002

© Copyright 2002 by VingCard 13:57:41 08/10/2002

Although you can use Change to change anything on an Employee Rooms keycard, normally it is used to extend the expiration date.

1. If the New Empl. Card screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Employee Rooms**.
2. Touch **Back** to display the **Empl. Room Cards** menu screen.
3. Select the **Room** number from the list on the left of the screen.
4. Touch **Change** and make any changes you need.
5. Touch **Encode**.

NOTE: After a few minutes of inactivity, the Login screen will be displayed and you will need to re-enter your password.

Removing Employee Rooms Keycards from the Vision System

About Removing an Employee Rooms Keycard

Most hotels will probably not need to use this feature for a couple of reasons:

- when a newer Employee Rooms keycard is used on a lock, any older keycards will no longer unlock the door
- Employee Rooms keycards automatically expire after the date and time that is encoded on the keycard

However, your hotel, may have reasons for wanting to use this. For example, some cruise ships will not be able to verify whether the employee has quit their room out unless they use the Remove Employee Card option.

If you are unsure of whether or not your hotel uses this feature, check with your hotel's Vision system administrator.

NOTE: Using the Remove Employee Card feature will not invalidate the Employee Rooms keycard, it will only indicate to the Vision system that the room is now vacant.

How to Remove Employee Rooms Keycards from the Vision System

This is similar to the Check Out feature in the Guest Keycards module.

1. If the New Empl. Card screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Employee Rooms**.
2. Touch **Back** to display the **Empl. Room Cards** menu screen.
3. Select the **Room** number from the list on the left of the screen.
4. Touch **Remove Empl. Card** to display the Replace Empl. Card screen.
5. If a list of cards is shown, select the card you want to remove (refer to dates, name tab etc). To check out the whole list, repeatedly press **Remove** then **Back** then **Remove empl. card**.
6. To select a different **Room** number, use the keypad on the right of the screen. Whenever you select a different room number, you will need to touch **Find** to update the screen with the new room number information.
7. Touch the **Remove** button. Any existing Employee Rooms keycards will still be valid, but they will be removed from the Vision database.

NOTE: After a few minutes of inactivity, the Login screen will be displayed and you will need to re-enter your password.

Viewing the Information on an Employee Rooms Keycard

About Viewing the Information on an Employee Rooms Keycard





Using the View Employee Card feature allows you to display the following information:

- Room number(s)
- Employee name
- User Group
- Whether the this keycard has access to Common doors

How to View the Information on an Employee Room Keycard

Viewing information about an Employee Rooms keycard is helpful, when hotel personnel wants to check if there are any cards (valid or pre-checked) issued to given room.

View empl. card

 Find
  Help
  Logout
  Back

Room





Keycard for

User group

Common doors

Cards

Cards found:

Name	Start date/time	End date/time	
<No name>	08/10/2002 11:52:0	10/10/2002 14:00:0	
			
			
			

© Copyright 2001, by VingCard

1. If the Empl. Room Card screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Employee Rooms**.
2. Touch **Back** to display the **Empl. Room Cards** menu screen.
3. Select a **Room**.
4. Touch **View**.

5. To view another room, enter the room number and touch **Find**.

Verifying the Information on an Employee Rooms Keycard

About Verifying the Information on an Employee Rooms Keycard

Using the Verify Employee Card feature allows you to “read” an Employee Rooms keycard and display the following information:





- Room number(s) that the keycard was made for
- Start date/time of the keycard
- Start/expiration date/time of the keycard
- User Group
- Keycard Type
- Whether the this keycard has access to Common doors
- Issue area

You can use **System Events** in the **Reports** module to determine which employee made the keycard.

NOTE: If you attempt to use the Employee Rooms module to Verify a blank keycard, a damaged keycard, a keycard made from a different module, or a keycard from a different hotel, an error message will be displayed.

How to Verify the Information on an Employee Room Keycard

Displaying information about an Employee Rooms keycard is helpful if an employee forgets his room number or a keycard is found.

<div>Verify empl. card</div>					
<div>Main</div> <div>Name</div> <div>Room</div> <div>201</div> <div>From date/time</div> <div>08/10/2002 13:16</div> <div>Until date/time</div> <div>10/10/2002 14:00</div> <div>User group</div> <div>Employee room</div> <div>Common doors</div> <div>No</div>	<div>Result</div> <div>More Data</div> <div>Keycard for</div> <div>flower delivery</div> <div>Issue area</div> <div>1</div> <div>Result</div> <div>Valid keycard.</div>				
© Copyright 2002 by VingCard		14:18:22 08/10/2002			

1. If the New Empl. Card screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Employee Rooms**.
2. Touch **Back** to display the **Empl. Room Cards** menu screen.
3. Touch **Verify**. You will be prompted to insert a keycard into the card reader.

TIP: For security purposes, the Card Encoder is set to wait for a brief period and if a keycard is not inserted, the process will be cancelled.
4. Examine the card information. To read another employee room keycard, touch **Verify** and insert the next keycard.

NOTE: If you attempt to use the Employee Rooms keycards module to Verify a blank keycard, a keycard made from a different module, or a keycard from a different hotel, an error message will be displayed.

Special Keycards Module



Special keycards

?
Help

✖
Logout

←
Back

Expiration dates

Fail-safe programming:
Valid until: 29/09/2004

Passage-mode:
Valid until: 29/09/2004

Void-list:
Valid until: 29/09/2004

Fail-safe

Verify

Passage-mode

Read-out

Lock-out

Service

Void-list

© Copyright 2002 by VingCard
14:49:43 08/10/2002

What the Special Keycards Module Does

	Description	Use this to
Fail Safe Cards	Pre-made guest keycards	Check in guests, even if the computer goes down.
Fail –safe Programming	Keycard that tells a lock to allow a Fail-safe keycard to be used.	Tell a lock to allow a Fail-safe keycard to be used. Must be used prior to using a Fail-safe keycard.
Lock-out / Undo Lock-out	Keycard that locks out an entire Guest User Group from a lock.	Prevent guests from returning to a room between the time they check out and the time their keycard expires. Undo Lock-out keycards reverse the action.
Passage-mode	Keycard that allows a door to remain unlocked after a valid employee / guest card is used.	Set up doors such that valid keycards can leave them unlocked, thereby allowing controlled access to rooms such as banquet halls.
Void-list	Keycard that invalidates up to 5 employee keycards for any lock it is used in.	Permanently prevent specific employees access to locks. Exclude up to 20 employees by using more than one Void-list keycard.

NOTE: For information on making a “One-shot” keycard to allow a door to be opened only once, refer to the Employee Rooms module.

Quick Guide to Using Special Keycards Module

This Help topic was designed as a quick reference. For more details on each task, touch the **Help** button and select the appropriate Help topic.

Task	Beginning from the Special Keycards menu screen:
Sequential Failsafe keycards	<p>TO MAKE KEYCARDS:</p> <ul style="list-style-type: none"> • Touch Fail-safe • Enter No. of keycards in stack (how many failsafe check ins to prepare for) • Enter Copies pr. Keycard (how many keycards per individual check in) • Choose a User Group • Touch Encode • Make cards as prompted. • Repeat to make enough sets for all rooms of hotel. <p>TO USE KEYCARDS:</p> <ul style="list-style-type: none"> • Use with Fail-safe Programming keycard now, at each door. • Give to guests as they check in.
Random Fail-safe keycards	<p>TO MAKE KEYCARDS:</p> <ul style="list-style-type: none"> • Touch Fail-safe • Enter 1 for No. of keycards • Enter 1 for Copies pr. Keycard • Choose a User Group • Touch Encode • Repeat to make enough keycards for all rooms of hotel. <p>TO USE KEYCARDS:</p> <ul style="list-style-type: none"> • When guest checks in, go to door and use with Fail-safe Programming keycard. • Give to guest.
Fail-safe Programming keycards	<p>TO MAKE KEYCARDS:</p> <ul style="list-style-type: none"> • Touch Fail-safe • Touch Programming tab. • Choose Yes or No for Override option • Touch Encode <p>TO USE KEYCARDS:</p> <ul style="list-style-type: none"> • See Sequential or Random Fail-safe keycard instructions.
Void-list Keycards	<p>TO MAKE KEYCARDS:</p> <ul style="list-style-type: none"> • Touch Void-list • Choose Yes or No for Override option • Use Add to select from Voided or Not voided list • Touch Encode <p>TO USE KEYCARDS:</p> <ul style="list-style-type: none"> • Insert in lock. Any employees listed on this keycard will no longer be able to open the lock.
Lock-out/Undo Lock-out Keycards	<p>TO MAKE KEYCARDS::</p> <ul style="list-style-type: none"> • Touch Lock-out • Select an employee to assign the keycard to • Choose one or more User Groups from Keycards list • Touch Encode

	<p>TO USE KEYCARDS:</p> <ul style="list-style-type: none"> • Insert keycard in lock. Any keycards with the User Groups listed on the Lock-out keycard will no longer be able to open the lock.
Passage-mode Keycards	<p>TO MAKE KEYCARDS:</p> <ul style="list-style-type: none"> • Touch Passage-mode • Choose Yes or No for Override option • Touch Encode <p>TO USE KEYCARDS:</p> <ul style="list-style-type: none"> • Insert in a lock. The next time the door is opened with a valid keycard it will remain <i>unlocked</i> until a valid keycard is used again to lock it. • Insert in the lock again. The door reverts to normal behaviour – the next time the door is opened with a valid keycard it will NOT remain <i>unlocked</i>.

Fail-safe Keycards

About Sequential and Random Fail-safe keycards

Fail-safe keycards are pre-made keycards, created so that if the computer ever goes down, you can use them as guest keycards.

You should always keep the Fail-safe keycards available, so if for any reason the computer is not working guests can still be issued with working keycards.

NOTE: Before a Fail-safe keycard can be used as a valid guest keycard, another special keycard called a Programming Fail-safe keycard must first be used on the lock. See the Help topic "About Programming Fail-safe Keycards" for more information.

There are two methods of implementing Fail-safe keycards:

Random – This method creates Fail-safe keycards that can be used for ANY door. At the actual time a guest checks in, you will need to use a Fail-safe Programming keycard and then a Fail-safe keycard on the door before giving the Fail-safe keycard to a guest.

Sequential – This method lets you create up to 8 Fail-safe keycards (plus duplicates) for each SPECIFIC guest room. Using this method, you activate each door with the Fail-safe Programming keycard and then a Fail-safe keycard just after making the cards. After that, the Fail-safe cards are ready to issue to guests if the computer system ever goes down. You do not have to use the Fail-safe Programming keycard at the time of check in.

	Advantages	Disadvantages
Random method	<p>Fast to create.</p> <p>No need for individually labelled sets of cards for each room :just one pile of Fail-safe cards (or even make them as guests arrive).</p> <p>No need to use Programming Fail-safe keycard until guests arrive.</p>	<p>As guests arrive, you will need to use the Fail-safe Programming keycard in each lock before using the guest's Fail-safe keycard (just made or picked from a pre-made pile).</p> <p>If there is a power outage, you may not have enough employees available to do this.</p> <p>If you did not pre-make enough Fail-safe keycards, you may quickly run out.</p> <p>If you need to make Fail-safe keycards as guests arrive, the front desk staff have to learn how (not the case with pre-made stacks).</p>

		Fail-safe Programming keycards need to be in circulation at check-in time. Maybe many copies to cope with demand. These can be used to open any lock.
Sequential method	<p>Check in is easier – just hand the guest their room key(s), picked from the specific Fail-safe card stack for their room.</p> <p>You will have enough Fail-safe keycards as they are pre-made for each specific room.</p> <p>Once the Fail-safe Programming keycard has been used it can be securely stored away as it is not needed at check in time.</p>	<p>Takes a little longer for initial set up as you will need to go to each room with the Fail-safe Programming keycard to activate the Fail-safe keycard stack for the room.</p> <p>You will need a clear system to label and group the Fail-safe cards for each specific room.</p>

NOTE: Unlike all other types of keycards, Random and Sequential Fail-safe keycards do not expire after 2 years.

About Fail-safe Programming keycards

Fail-safe Programming keycards instruct a lock to allow Fail-safe keycards to be used as guest keycards.

They are always used as the first part of a two-step process, with Fail-safe keycards. First, the Fail-safe Programming keycard is inserted to tell the lock to allow a Fail-safe keycard to work. Then a Fail-safe keycard is inserted. At this point, the Fail-safe keycard becomes a valid guest keycard – and if a stack of sequential Fail-safe cards was made, the rest of the stack become valid ‘future’ guest cards for that specific room.

If you are using Random Fail-safe keycards, you will not use the Fail-safe Programming keycard until you check in guests. If you are using Sequential Fail-safe keycards, you will use the Fail-safe Programming keycard on each room at the time the Sequential Fail-safe keycards are made, so that in the event of a crisis, guests can be checked in without any unwelcome last minute effort.

You should always keep the Programming Fail-safe keycard available in the event that the computer is down.



WARNING! Anyone with a valid Fail-safe keycard and the Programming Fail-safe keycard potentially could gain access to any door, so be certain to store the Fail-safe Programming keycard in a secure place.

NOTE: Programming Fail-safe keycards expire 2 years from the date they were created. Always make a new Programming Fail-safe keycard before the old one expires.

How to Make Fail-safe Programming keycards

The screenshot shows the 'Fail-safe' programming interface. At the top, there's a navigation bar with a 'Fail-safe' button, an 'Encode' button, and 'Help', 'Logout', and 'Back' buttons. Below this, there are two tabs: 'Fail-safe' and 'Programming'. The 'Fail-safe' tab displays 'Keycard information' with 'Current keycard valid until: 29/09/2004'. The 'Programming' tab displays 'Override previous keycard(s)' with two options: 'Yes' (unchecked) and 'No' (checked). The bottom status bar shows '© Copyright 2002 by VingCard', the time '08:50:19', and the date '09/10/2002'.

1. If the main Special Keycards screen is not displayed, touch **Back** to return to the Vision **Main** menu, touch **Special Keycards** then **Fail-safe**.
2. Touch the **Programming** tab to display the **Fail-safe Programming** screen. The expiration date of the Fail-safe keycards will be displayed.
3. **Override previous keycards:**
 Choose **Yes** if this is the first Fail-safe Programming keycard for the system, or if you need make new Fail-safe cards and the expiry date is approaching. Also choose **Yes** if you have lost the original Fail-safe Programming keycard. Choose **No** if you want to make a duplicate Fail-safe Programming keycard – for example so that 2 people can share the task of setting up rooms for sequential Fail-safe cards.
*If you choose **Yes**, any currently valid Fail-safe Programming keycards will not function in the locks after the newer Fail-safe Programming keycard is used on them. The new keycard will be valid for 2 years from the time it was made.*
*If you choose **No**, a copy of the newest version of the Fail-safe Programming keycard will be made. The previous Fail-safe Programming keycard will continue to work and they will both expire 2 years from the date that the first one was made.*
4. Touch **Encode**
5. When prompted, insert a keycard into the encoder. Notice that the expiration date on the left side of the screen is updated if you chose **Yes** in Step 3.

NOTE: Programming Fail-safe keycards should be stored in a safe place as they can be used in conjunction with Sequential or Random Fail-safe keycards to unlock virtually any door.

How to make Random Fail-safe keycards

The screenshot shows the 'Fail-safe' programming interface. It includes a top navigation bar with 'Fail-safe' and 'Programming' tabs, and buttons for 'Encode', 'Help', 'Logout', and 'Back'. The 'Fail-safe' tab is selected, displaying input fields for 'No. of keycards in stack' (set to 1), 'Copies pr. keycard' (set to 1), and 'User group' (set to 'Regular Guest'). To the right is a list of 'User groups' with 'Regular Guest', 'V.I.P Guest', and 'Employee room'. Each group has a corresponding icon button. The bottom status bar shows '© Copyright 2002 by VingCard', the time '09:17:33', and the date '09/10/2002'.

1. If the main Special Keycards screen is not displayed, touch **Back** to return to the Vision **Main** menu, touch **Special Keycards** then **Fail-safe**.
2. Leave the **No. of keycards in stack** set to one.
3. Leave the **Copies pr. Keycard** set to one.
4. Touch the current setting for **User group** and then select the User group that you want to make keycards for. If you are unsure of which User group to select, check with your hotel's Vision system administrator.

TIP: *Each hotel creates its own User groups for guests based on the hotel's needs, so your hotel may have more than one. However, it is recommended that there be a "generic" user group that can be selected for Fail-safe keycards so that you do not have to repeat the entire process of creating Fail-safe keycards for each guest User group in the system.*

5. Touch the **Encode** button. You will see the message "Insert Keycard, Card #1 Copy #1". Insert a keycard into the encoder.
6. You will be returned to the **Fail-safe** screen. Repeat Step 5 for each guest room in the hotel. For example, if your hotel has 100 rooms it is sensible to make (at least) 100 Fail-safe cards.
7. Store the pile of Fail-safe cards somewhere accessible.

8. When a guest checks into the hotel, go to their door and insert a Fail-safe Programming keycard and then any one of the Random Fail-safe keycards. You can then give the Fail-safe keycard to the guest.

NOTE: Room numbers for Fail-safe keycards are not assigned to the keycard until they are used at the door after the Fail-safe Programming keycard.

How to make Sequential Fail-safe keycards

The screenshot shows the 'Fail-safe' programming interface. It includes a numeric keypad for entering values and a 'User group' dropdown menu. The current settings are 8 keycards in stack, 2 copies per keycard, and the 'Regular Guest' user group.

1. If the main Special Keycards screen is not displayed, touch Back to return to the Vision Main menu, touch **Special Keycards** then **Fail-safe**.
2. Use the number pad on the right side of the screen to enter the **No. of keycards in stack**. This number determines how many *times* you will be able to check new guests into each room using Fail-safe keycards.
TIP: *Each hotel creates its own User groups for guests based on the hotel's needs, so your hotel may have more than one. However, it is recommended that there be a "generic" user group that can be selected for Fail-safe keycards so that you do not have to repeat the entire process of creating Fail-safe keycards for each guest User group in the system.*
3. Touch the current setting for **Copies pr. keycard** and then use the number pad on the right side of the screen to enter the number of copies (Duplicate keycards) you want to make of each keycard for each set.

TIP: *As an example, assume that:
You have entered 3 for No. of keycards in stack
You have entered 2 for **Copies pr. Keycard**
Your hotel has 100 guest rooms
You would make a total of 600 keycards and would be able to make three separate check ins using Fail-safe Sequential keycards. Each time you check in a guest, you would have 2 valid keycards for the room – for roommates / family members.*

4. Touch the current setting for **User group** and then select the User group that you want to make keycards for. If you are unsure of which User group to select, check with your hotel's Vision system administrator.

TIP: *Each hotel creates its own User groups for guests based on the hotel's needs, so your hotel may have more than one. However, it is recommended that there be a "generic" user group that can be selected for Fail-safe keycards so that you do not have to repeat the entire process of creating Fail-safe keycards for each guest User group in the system.*

5. Touch the **Encode** button. You will see the message "Insert Keycard, Card #1 Copy #1". Insert the first keycard into the encoder.
6. Follow the prompts onscreen to make further cards. Carefully group the cards as they are made.

Using our previous example (cards in stack = 3, copies = 2):

- Card #1 Copy #1
- Card #1 Copy #2
- group copy 1 & 2 together (elastic band or similar)
- Card #2 Copy #1
- Card #2 Copy #2
- group copy 1 & 2 together (elastic band or similar)
- Card #3 Copy #1
- Card #3 Copy #2
- group copy 1 & 2 together (elastic band or similar)
- Place the 3 sets in an envelope (or similar).

At this point you have made **all** of the Fail-safe keycards for **one** room. Place this set into an envelope, keeping duplicates together (copy 1 and copy 2 for each card). The actual room numbers will not be assigned to the keycards until Step 10.

7. Repeat steps 5 & 6 for each guest room in the hotel. You will now have many envelopes, each containing a set of cards.
8. Take the Fail-safe Programming keycard and a set (envelope) of Sequential Fail-safe keycards to a guest room.
9. Use the Fail-safe Programming keycard on the lock
10. Remove any one of the keycards from a set (envelope) and insert it into the lock. You will see a green flash on the lock (but it will not open). This assigns the room number to the entire set. None of the other copies in the set need to be used at this time.
11. Return the keycard to the envelope (with its own specific duplicates if it had any). Mark the envelope with the room number. (You could have written the room numbers on the envelopes as you made the sets)
12. Repeat steps 8 thru 11 for all rooms at the hotel, using a new set (envelope) of cards for each room.
13. Take all your envelopes back to reception area and store the cards in an

orderly manner such that they can be used when required. Lock all Fail-safe Programming keycards that were used during the process in a secure place.

REMEMBER: Room numbers for Fail-safe keycards are not assigned to the keycard until they are used at the door with the Fail-safe Programming Fail-safe keycard.

Lock-out and Undo Lock-out Keycards

About Lock-out and Undo Lock-out keycards

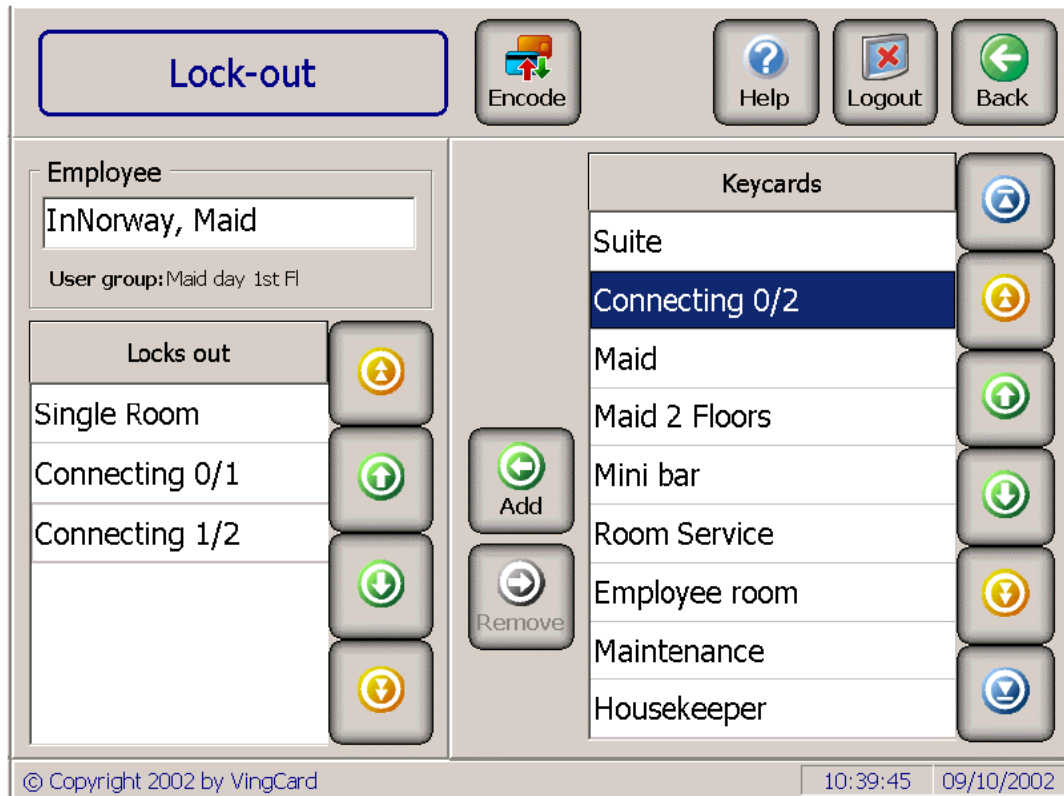
Lock-out keycards are issued to specific employees (usually maids) and they are normally used to prevent guests from returning to a room between the time they check out and the time their keycard expires.

When the room is cleaned, the maid can use the Lock-out keycard on the door. Then, only new guests will be able to open the door. This will ensure that the room will remain clean until the new guest checks in.

Whenever a Lock-out keycard is made, an **Undo Lock-out** keycard is also made. The Undo Lock-out keycard reverses the action of the Lock-out keycard and is normally only used if the guest has not actually checked out.

NOTE: Normally, Lock-out keycards are not used to prevent a specific problematic guest from accessing their room. An easier way to accomplish this would be to make a new keycard for their room and use it on the lock so that their old keycard will no longer open the door. When the problem is resolved, you can just make them the new keycard, but if you had used a Lock-out keycard, you would need to send an employee back to the room with an Undo Lock-out keycard.

How to make Lock-out and Undo Lock-out keycards



1. If the main Special Keycards screen is not displayed, touch **Back** to return to the Vision **Main** menu, touch **Special Keycards**.
2. Touch **Lock-out** to display the **Lock-out** screen.
3. Select a name from the **Employee** window on the right side of the screen. The keycard will be assigned to this person.
4. Touch the **Locks out** window to display the **Keycards** list on the right side of the screen.
5. Touch the type of keycard you want to lock out and touch **Add**. Repeat for all keycard types you wish to lock out (normally, each guest keycard type).
6. Touch the **Encode** button to make the keycards. You will be prompted to insert a keycard as a Lock-out keycard and then a keycard as an Undo Lock-out keycard.
7. Label and give the keycards to the selected employee.
8. To make lockout cards for other employees, touch the **Employee** window, select another employee and repeat the process (3 thru 7).

Passage Mode Keycards

About Passage-Mode keycards

Using a Passage-mode keycard on a door does not actually lock or unlock it, but causes the door to enter Passage Mode. In this mode, the next time the door is opened with a valid keycard it will remain unlocked until a valid keycard is used again to lock it.

The lock will remain in passage mode, switching between locked and unlocked with every valid keycard insertion, until the Passage-mode keycard is used again. Then, the door reverts to normal behaviour - the next time the door is opened with a valid keycard it will NOT remain unlocked.

Passage-mode keycards are not made for a specific door, but can be used on ANY door.

Normally, Passage-Mode keycards are used for situations such as parties in banquet rooms or meetings in conference rooms when you want to allow the door to remain unlocked for a period.



WARNING! Passage-mode keycards will work on all doors, so store it in a safe place for security reasons.

How to make Passage-Mode keycards

The screenshot shows the 'Passage mode' configuration window. At the top, there is a title bar with a button labeled 'Passage mode'. To the right of the title bar are four buttons: 'Encode' (with a keycard icon), 'Help' (with a question mark icon), 'Logout' (with a red X icon), and 'Back' (with a green left arrow icon). The main area is divided into two panels. The left panel, titled 'Keycard information', contains the text 'Current keycard valid until: 29/09/2004'. The right panel, titled 'Override previous keycard(s)', contains two radio buttons: 'Yes' (which is selected) and 'No'. At the bottom of the window, there is a status bar with the copyright notice '© Copyright 2002 by VingCard' on the left, and the time '11:11:48' and date '09/10/2002' on the right.

Passage mode	
Keycard information Current keycard valid until: 29/09/2004	Override previous keycard(s) <input checked="" type="radio"/> Yes <input type="radio"/> No

© Copyright 2002 by VingCard 11:11:48 09/10/2002

1. If the main Special Keycards screen is not displayed, touch **Back** to return to the Vision **Main** menu, touch **Special Keycards**.
2. Touch **Passage-mode** to display the **Passage-mode** screen. The expiration date of the Passage-mode keycards will be displayed.
3. For **Override previous keycards**:
Choose **Yes** if this is the first Passage Mode keycard for the system, or if you need to renew your Passage Mode card because the expiry date is approaching. Also choose **Yes** if you have lost the original Passage Mode keycard.
Choose **No** if you want to make a duplicate Passage Mode keycard– for example so that 2 staff members can have one.
*If you choose **Yes**, any currently valid Passage-mode keycards will no longer function in the locks after the new Passage-mode keycard is used on them. The new keycard will expire 2 years from the time it was made.*
*If you choose **No**, the new Passage-mode keycard will not affect any currently valid Passage-mode keycards. They will both expire 2 years from the date that the first one was made.*
4. Touch the **Encode** button.
5. When prompted, insert a keycard into the encoder. Notice that the expiration date on the left side of the screen has changed only if you chose **Yes** for Step 3.

<p>NOTE: Passage-mode keycards should be stored in a safe place as they can cause any door they are used on to remain unlocked for long periods.</p>
--

Void-list Keycards

About Void-list keycards

The Void-list allows you to remove the access of up to 20 **employee** keycards from a lock. You may wish to do this to prevent lost employee keycards from being used, or if an employee leaves the hotel without turning in their keycard.

Unlike Lock-out keycards, individual employees are removed from access rather than an entire User Group.

The Vision system can contain a Void-list of up to 20 employees. Each Void-list **keycard** can contain up to 5 employees. Therefore, you need to create more than one Void-list keycard if you want to remove access for more than 5 employees.



WARNING! If you want to remove an employee from the Vision system as well as from a Void-list, you **MUST** remove them from the Void-list first.

NOTE : You can prevent a single employee card being used as follows :

- Go to employee keycards module. Select the employee name and encode a new keycard.
- Use this keycard in all locks the employee had access to. This will ensure that the lost / not turned in keycard can no longer open these doors.
- Destroy the new keycard.
- Remove the employee record (employee keycards module) if desired.

The advantage of the void list card is that you can block access for many employees in a single visit to a lock.

How to make Void-list keycards

1. If the main Special Keycards screen does not display, touch **Back** to return to the Vision **Main** menu, touch **Special Keycards**.
2. Touch **Void-list** to display the **Void-list** screen.
3. **Override previous keycards:**
 If you choose **Yes**, when this keycard is used, the Void-list within the lock will be replaced by the new list on the keycard. The new keycard will expire 2 years from the time it was made.
 If you choose **No**, when this keycard is used, the names on this keycard will be added to the list within the lock. They will both expire 2 years from the date that the first one was made.
4. Touch the **Not voided** tab to display a list of employees who are not in the system Void-list.
 OR
 Touch the **Voided** tab to display a list of employees who have already been added to the system Void-list.
5. Touch either the **Employee name** or **Employee Id** tab to sort the list by name or ID number.
6. Touch the employee name and use **Add** and **Remove** to move names to and from the Voids window.

A **plus** sign after a name in this window indicates that this employee will become Voided. A **minus** sign indicates the employee will become Not

voided (that is, have their voided status overturned).

When the Void-list keycard is used on the lock, employees with a **plus** sign after their names, will not be able to open it with their keycards. Any employees with a **minus** sign will now have their access restored if they still have a valid employee keycard.

7. Touch the **Encode** button and insert the keycard when prompted on the screen.

Read-out cards

About Readout keycards

A special Smart card called a Read-out keycard can be used to download events from locks. The Read-out keycard is used only for reading events from a lock. It does not unlock any doors. When you insert the Read-out keycard to the lock, the lock software copies the events from the lock memory to a log file on the keycard. The event information can then be transferred to the Vision system and viewed and printed via the **Reports** module.

You can make as many readout cards as you require. Each read-out card can only hold information from one lock at a time : if you use the card on more than one lock, only the information of the last lock is stored on the card. When you read information from a lock using a Read-out keycard, the signal light on the lock flashes yellow during the event download and a short green flash when the download is complete. Do not remove the card until the yellow LED light is off.

Read-out cards must be Smart cards and can only read events from VingCard locks that accept Smart cards. (Make a Setup / Locktypes report from the Reports module to see which locks accept Smart cards).

NOTE : Lock events can also be downloaded to the Vision system (from ANY lock type) using the Pocket PC LockLink – see chapter 4.

How to make Readout keycards

1. If the main Special Keycards screen does not display, touch **Back** to return to the Vision **Main** menu, touch **Special Keycards**.
2. Touch **Read-out** button
3. Encode a Smart card when prompted.
4. Use the card to download events from a lock, then use the Vision Reports module to transfer the events from the read-out card to the Vision system. You can then view and print the events from the Reports module. The readout card can then be re-used in another lock.

Service keycards

About Service keycards

A special Smart card called a Service keycard can be used to download maintenance and statistical information from locks. The Service keycard is used only for reading events from a lock. It does not unlock any doors. When you insert the Service keycard into the lock, the lock software copies service data to the keycard. The service information can then be transferred to the Vision system and viewed and printed via the **Reports** module.

You can make as many Service cards as you require. Each read-out card can only hold information from one lock at a time : if you use the card on more than one lock, only the information from the last lock is stored on the card

Service cards must be Smart cards and can only read data from VingCard locks that accept Smart cards. (Make a Setup / Locktypes report from the Reports module to see which locks accept Smart cards).

How to make Service keycards

1. If the main Special Keycards screen does not display, touch **Back** to return to the Vision **Main** menu, touch **Special Keycards**.
2. Touch **Service** button
3. Encode a Smart card when prompted.
4. Use the card to download data from a lock, then use the Vision Reports module to transfer the data from the service card to the Vision system. You can then view and print the information from the Reports module. The service card can then be re-used in another lock.

Verifying Special Keycards

About Verifying the Information on Special Keycards

Using the Verify Special Card feature allows you to “read” a Special keycard and display the following information:

- Type of card
- Start date/time of the keycard
- Start/expiration date/time of the keycard
- Whether the card is currently valid
- Extra information (dependent on special card type)

You can use **System Events** in the **Reports** module to determine which employee made the keycard.

NOTE: If you attempt to use the Special Cards module to Verify a blank keycard, a damaged keycard, a keycard made from a different module, or a keycard from a different hotel, an error message will be displayed.

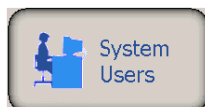
How to Verify the Information on a Special keycard

Voided Employees		
Muscles, Mandy	s100	+
Troy, Helen	m102	+

© Copyright 2002 by VingCard 11:49:28 09/10/2002

1. If the **Special Keycards** screen is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **Special Keycards**.
2. Touch **Verify**. You will be prompted to insert a keycard into the card reader.
3. Examine the card information. To read another special keycard, touch **Verify** and insert the next keycard.

System Users Module



Name	Id	System access
Mellie, Roger	f100	Front office
VingCard, Demo1	VingCard 1	VC Supervisor
VingCard, Demo2	VingCard 2	VC Supervisor
Welsh, Trevor	W345	Management

© Copyright 2002 by VingCard 13:42:23 09/10/2002

What the System Users Module Does

The System Users module allows you to give employees access to some or all of the Vision system modules.

When you add an employee to this module, they will be assigned a unique password. The Vision Login screen will require the employee to enter this password before allowing them to access any of the Vision modules.

NOTE: The Employee Keycards and System Users modules share the same employee information. Therefore using Add or Change from either, automatically update the other.

Quick Guide to Using the System Users Module

This Help topic was designed as a quick reference. For more details on each task, touch the **Help** button and select the appropriate Help topic.

Task	Beginning from the System Users screen:
Making an employee who does not already have a keycard a system user	<ul style="list-style-type: none"> • Touch Add (New tab is selected) • Touch the keyboard button for Employee Id. And enter the information • Touch Enter to return to the Add employee screen. • Repeat steps 2 and 3 for Last name and First name • Touch System access and make a selection

	<ul style="list-style-type: none"> • Touch the Password button. Define your own username and password, or read the automatically generated password (depending on set up). • Touch Save
Making an employee who already has a keycard a system user	<ul style="list-style-type: none"> • Touch Add • Touch Keycard Holder tab • Touch the name of the employee from the list on the right side of the screen • Touch System access and select one • Touch the Password button. Define your own username and password, or read the automatically generated password (depending on set up). • Touch Save
Changing Employee Information or Access rights	<ul style="list-style-type: none"> • Touch the name of the employee from the list on the right side of the screen • Touch Change • Make any changes • Touch Save
Removing an employee's System Access	<ul style="list-style-type: none"> • If the employee is on a Void-list, remove them from it • Touch the name of the employee you want to Remove • Touch Remove • Touch Yes

Assigning Access to Employees

About Assigning Access to employees

Before you can give an employee access to any of the modules, you must Add the employee to the System Users module. To do this you can either enter new information or select employee information that was entered in the Employee Keycards module.

To simplify the process of assigning access to employees, your hotel has (via the Vision setup module) created **System Access Groups**. Choosing one of these groups for the employee will determine which modules they will have access to.

You can give an employee access to some or all of the Vision modules. Any modules they do not have access to will be “greyed out” on the **Main** menu.

NOTE: The Employee Keycards and System Users Modules share the same employee name and ID information.

How to add an Employee who does not already have a keycard

1. If the main System Users screen is not displayed, touch **Back** to return to the Vision **Main** menu, touch **System Users**.
2. Touch **Add** to display the **Add employee** screen. The **New** tab will already be selected.
3. Enter the Employee ID, Last name and First name.
4. Touch the **System access** window and select a System Access Group from the list that appears on the right of the screen.
If you are unsure of which System access group to select, check with your hotel's Vision system administrator.
5. Touch the **Password** button. Depending on your system setup this will either say 'New Password' or 'Set Username and Password'.
If a numeric password is automatically displayed, note it down.
If for any reason, you don't like the password number that appears, you can press the Password button again to assign a different one.
If you are prompted to define a Username and Password, then do so (or let the employee in question do so). The password must be at least 4 characters long. You will need to re-enter the password to confirm it.
TIP: The login username will default to the Employee ID that you entered. However, you can change it if you wish. The login Username can **ONLY** contain letters and numbers, not special characters such as _ - * or ?
6. Touch **Save** to save the information. Logout and test the password.

Username is not case sensitive : password is.

Adding an Employee that has Been Issued an Employee Keycard

Add system user

Save Help Logout Back

New Keycard holders

Employee Id
m102

Last name
Troy

First name
Helen

System access
Front office

Set Username and Password

Login Username
m102

New password

Confirm new password

© Copyright 2002 by VingCard 13:35:53 09/10/2002

1. If the main System Users screen is not displayed, touch **Back** to return to the Vision **Main** menu, touch **System Users**.
2. Touch **Add** to display the **Add employee** screen. The **New** tab will be selected. Touch **Keycard Holders** tab.
3. Select an employee from the list on the right.
4. Touch the **System access** window and select a System Access Group from the list that appears on the right of the screen.
If you are unsure of which System access group to select, check with your hotel's Vision system administrator.
5. Touch the **Password** button. Depending on your system setup this will either say '**New Password**' or '**Set Username and Password**'.
If a numeric password is automatically displayed, note it down.
If for any reason, you don't like the password number that appears, you can press the Password button again to assign a different one.
If you are prompted to define a Username and Password, then do so (or let the employee in question do so). The password must be at least 4 characters long. You will need to re-enter the password to confirm it.

TIP: *The login username will default to the Employee ID that you inherited from the employee keycards module. However, you can change it if you wish. The login Username can ONLY contain letters and numbers, not special characters such as _ - * or ?*

- 6.** Touch **Save** to save the information. Logout and test the password.
Username is not case sensitive : password is.

Changing System User information for an employee

About Changing system user information

You can change ANY of the employee information, defined in the System Users module including their access and password.

If you have selected a new password scheme in the Vision setup module (Setup > System Access > Login) you can upgrade the passwords of all system users.

NOTE: The Employee Keycards and System Users modules share the same employee name and ID information. Therefore, any changes you make in the System Users module will automatically update the Employee Keycards module.

How to Change system user information for an employee

1. If the main System Users screen is not displayed, touch **Back** to return to the Vision **Main** menu, touch **System Users**.
2. Touch the name of the employee you want to Change information for.
3. Touch **Change** to display the Change System User screen.
4. If you want to change Employee ID or a name, enter the new information.
4. If you want to change System Access, touch the **System Access** window and select from the list that appears on the right of the screen.

If you are unsure of which System access group to select, check with your hotel's Vision system administrator.

5. If you want to change the Password – maybe you are upgrading all system users to a more secure password scheme - touch the **Password** button. Depending on your system setup this will either say '**New Password**' or '**Set Username and Password**'.

If a numeric password is automatically displayed, note it down.

If for any reason, you don't like the password number that appears, you can press the Password button again to assign a different one.

If you are prompted to define a Username and Password, then do so (or let the employee in question do so). The password must be at least 4 characters long. You will need to re-enter the password to confirm it.

TIP: *The login username will default to the Employee ID. However, you can change it if you wish. The login Username can ONLY contain letters and numbers, not special characters such as _ - * or ?*

6. Touch **Save** to save the information.

<p>NOTE: If this employee has been added to the Employee Keycards module, it will be updated by any changes you make to name or employee ID.</p>
--

Removing System Access from an Employee

About Removing and Employee from the System Users module

Removing employees from the system user module removes their system access to all Vision modules. If employees have not been issued an employee keycard, their information will be Removed completely from the Vision system. If they have been issued a keycard, you will need to use the Employee to remove the record of their keycard from the system.

How to Remove an Employee From the System Users Module

<p>NOTE: If this employee has been issued a keycard, they will not be removed from the Employee Keycards module.</p>
--

1. If the employee is on a Void-list, remove them from it.
 2. If the main **System Users** screen does not display, touch **Back** to return to the Vision **Main** menu, touch **System Users**.
 3. Touch the name of the employee you want to Remove.
 4. Touch **Remove**.
 5. A message will appear asking you to confirm the deletion.
-



Touch **Yes**. This process means the employee can no longer log in to Vision, but does not invalidate the employee's keycard if they have one.

6. You will be returned to the **System Users** menu screen.

Viewing Employee Information

About Viewing Employee Information

Both the Employee Keycards and the System Users modules allow you to display employee information.

The following information can be viewed from the System Users module:

- Employee ID
- Name
- System Access Group that the employee is assigned to

NOTE: To print a list of all employees, refer to the Reports module.
--

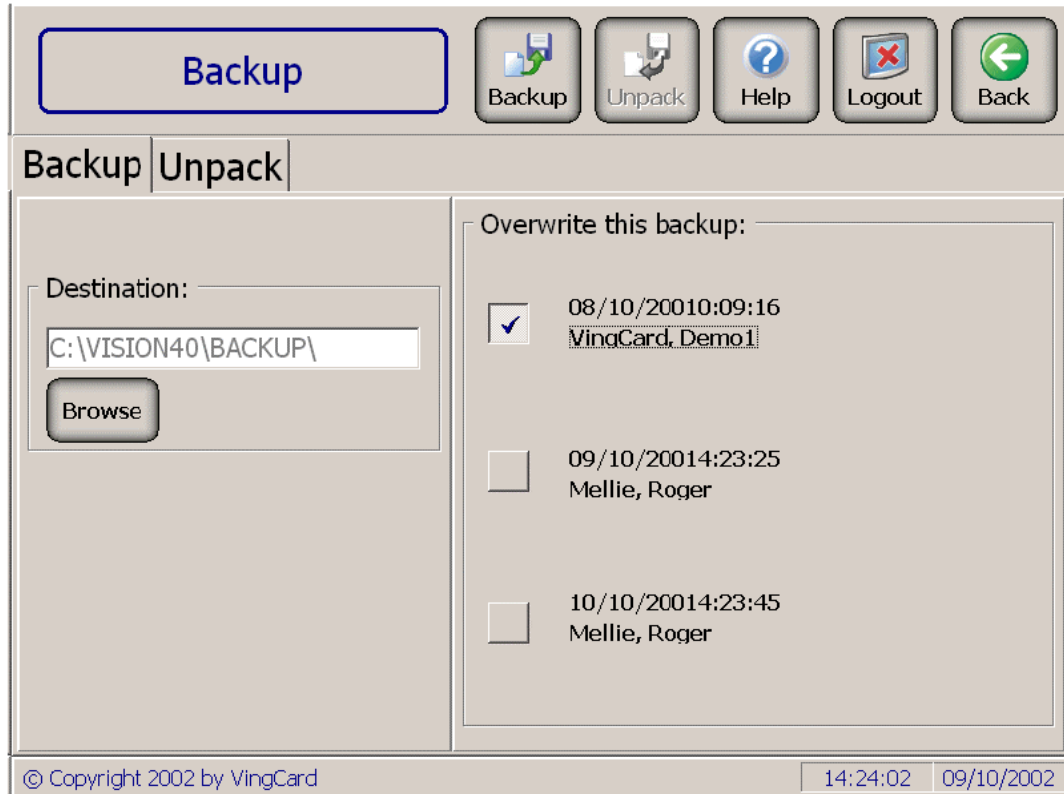
How to View Employee Information

1. If the main **System Users** screen is not displayed, touch **Back** to return to the Vision **Main** menu, touch **System Users**. The name and Employee ID of all employees with system access will be listed. Click on one of the column headers (Name, Id, System Access) to sort as you wish.

NOTE: To print a list of all employees, refer to the Reports module.
--

If you have the employee keycard in your possession, you can use Verify from the Employee Keycards module to display the information on it.

Backup Module



What the Backup Module Does

The Backup module allows you to back up and restore your Vision system data. The module has two parts: Backup and Unpack.

The Backup part lets you manually backup your Vision system data. The Vision system allows you to keep 3 different versions of your manual backup on the server system or as many versions as you wish on floppy diskettes.

The Unpack part is used when you want to restore your Vision system data. It allows you to select which backup version you want to use for the restore, unpacks it and prepares it to be restored. The data is restored to the Vision database by a separate executable, Restorer.exe which can be run very quickly from the windows programs menu.

You should use Backup so that in the event that your Vision system data ever becomes corrupted or is removed from the Vision database, you can get the data back.

The Vision system offers two different backup features: Manual backup from the Maintenance module and Autobackup from the System Setup module. The Autobackup version of your Vision system data is kept in addition to the 3 versions of the manual backup. To unpack and restore the Autobackup of your data, follow the instructions in this section.

For more information about the Autobackup feature, please refer to the documentation for the System Setup module or the online help system.

NOTE: You may never need to use the backups, but it is strongly recommended that you use the autobackup feature in setup to make a daily backup and also use the Backup module regularly in order to save data to a physically separate location (floppy disks or another PC on the network).

Quick Steps to using the Backup Module

This Help topic was designed as a quick reference. For more details on each task, touch the **Help** button and select the appropriate Help topic.

Task	Beginning from the Maintenance screen:
Making backups	<ul style="list-style-type: none"> • Touch the Backup tab to display Backup screen. • Enter a Destination directory for the backup. Browse to the desired destination. If you wish to store the backup on a diskette, browse to drive A (or appropriate) and insert a diskette. • Touch Backup button
Unpacking a backup	<ul style="list-style-type: none"> • Touch the Unpack tab to display Unpack screen. • Browse to the destination where the backup will be fetched from. If you wish to store the backup on a diskette, browse to drive A (or appropriate) having first inserted the backup diskette #1. • Touch Unpack button

How to Backup Data

All Vision PCs can be on and in use during backup!

1. If the main Backup screen is not displayed, touch **Back** to return to the Vision **Main** menu, touch **Backup**.
2. Touch the **Backup** tab.
3. Enter a **Destination** directory for the backup. Touch the **Browse** button if you wish to browse to the desired destination. If you wish to store the backup on a diskette, browse to drive A (or appropriate) and insert a diskette.

TIP: *If you are backing up to Floppy diskettes, it is recommended that you label the diskettes to indicate the date of the backup and the number the diskettes within the set.*

For example, if this set requires 4 diskettes, label the first diskette "Aug. 24, 2000 – Disk 1 of 4" and so on.

4. Touch the tick box in front of the backup you want to **Overwrite** (replace) with the new backup.
5. Touch the **Backup** button.

How to unpack data that has been backed up

The screenshot shows the 'Unpack' screen of the VingCard Vision 4.1 interface. At the top, there is a navigation bar with buttons for 'Backup', 'Unpack', 'Help', 'Logout', and 'Back'. Below this, the 'Unpack' tab is selected. On the left, there is a 'From:' field with the text 'C:\VISION40\BACKUP\' and a 'Browse' button. On the right, under the heading 'Unpack this backup:', there is a list of backup entries, each with a checkbox and a description:

Checkbox	Date/Time	Description
<input type="checkbox"/>	08/10/20010:09:16	VingCard, Demo1
<input checked="" type="checkbox"/>	09/10/20014:23:25	Mellie, Roger
<input type="checkbox"/>	10/10/20014:23:45	Mellie, Roger
<input type="checkbox"/>	26/06/20025:20:19	Auto, Backup

At the bottom of the screen, there is a status bar with the text '© Copyright 2002 by VingCard' on the left, and the time '14:25:30' and date '09/10/2002' on the right.

1. If the main **Backup** screen is not displayed, touch **Back** to return to the Vision Main menu, touch **Backup**.
2. Touch the **Unpack** tab.
3. Choose where the backup should be unpacked **from**. Touch the **Browse** button if you wish to browse to where the backup is. If the backup is on a diskette, browse to the diskette drive having inserted the diskette.
5. Touch the box in front of the backup you want to **Unpack**.
6. Touch the **Unpack** button when you are finished making changes to the screen.
7. Touch the OK button when the message “**To complete the database restore, use the program Restorer.exe!**” appears on the screen.
8. To complete the database restore, select Restorer from the VingCard Vision section of the start menu, then follow the step by step instructions presented on-screen (further details follow).

How to restore a backup using Restorer



WARNING!

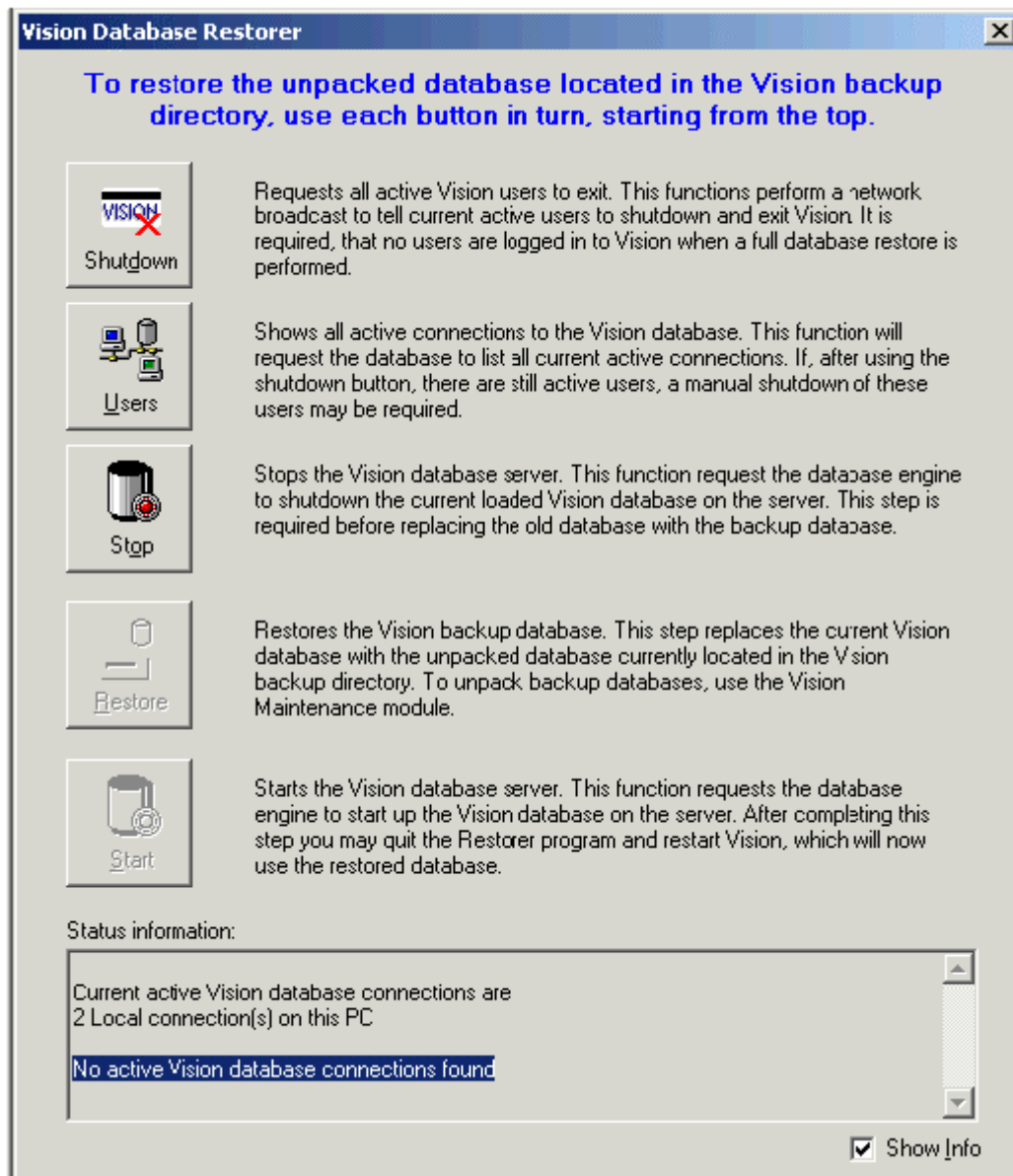
All users must exit the Vision system before a restore can occur.




The restore tool Restorer, guides you through the restore process. Before you start Restorer, make sure you have unpacked a backup. Backups are unpacked using Unpack feature in the Backup module.



How to restore unpacked backup data

1. Unpack the backup you want to restore (see previous instructions).
This will create an unpacked database (vision.db) in the /backup folder on the Vision server PC.
2. Start the program Restorer.exe. Start > Programs > VingCard > Vision > Restorer.
3. Follow the instructions on the screen and perform the five steps in the restore process.

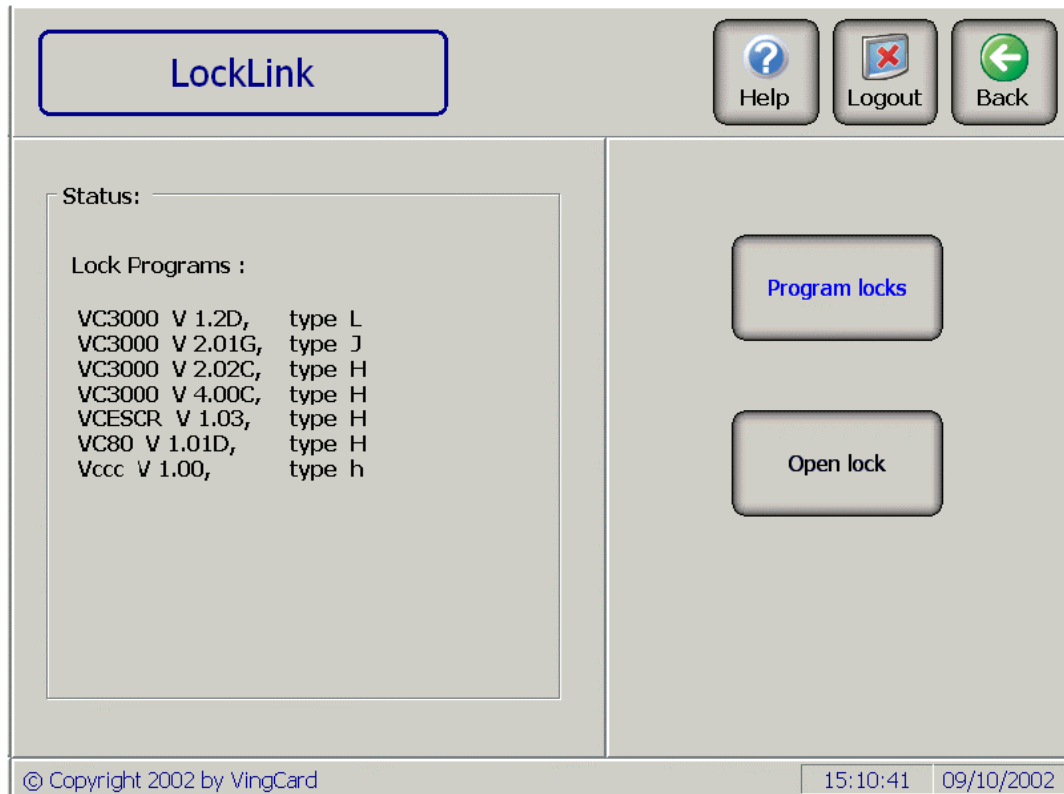
The Restorer screen



Button	Description
	Touch this button to broadcast a message requesting all users to exit the Vision system.
	Touch this button to view a list of users still connected to the database server. You should only proceed when the status message says ' No active Vision database connections found '
	Touch this button to shutdown the current loaded Vision database on the server. This step is required to complete the restore process.

 Restore	<p>Touch this button to start the actual restore. This step replaces the current Vision database with the unpacked database currently located in the server ..\ backup folder.</p>
 Start	<p>Touch this button to start the Vision database server when the restore is complete. The data in the database is now the data which was stored in the backup. This step is required to let users log back into Vision.</p>

LockLink Module



Programming Locks

About Programming Locks

Whenever a keycard is inserted in a lock, the lock must determine whether this keycard should be allowed to open the door. Each lock must be “programmed” to give it this information.

This information is contained in the Vision system. The LockLink is used to transfer this information from the Vision system (using the LockLink module) to the locks (using the Contact Card).

The LockLink itself is a Pocket PC used to communicate with the Hotel locks. It can :

- Interrogate a lock to extract details about entry events – the results can be displayed on the LockLink or transferred to a Vision PC
- Program locks by transferring information to them from the LockLink module of the Vision system – this includes resetting the date and time as well as changing the behaviour of the lock
- Unlock any door – even if the lock's battery is too low to open the lock

LockLinks are delivered to you with all of the necessary software installed on them. For more information about the LockLink, read Chapter 4 of this manual.

About Changing the programming of a lock

Whether a lock is being programmed for the first time, or being reprogrammed, the process is the same;

- the current information is extracted from the database and sent to from the LockLink module to the LockLink Pocket PC
- the VingCard LockLink software is run on the LockLink Pocket PC
- the necessary information is loaded into the lock using a Contact Card attached to the Pocket PC and inserted into the lock.

There are several instances when you might want to reprogram a lock:

- To change or add functionality – for example, a lock you may want to change a lock so that it can be used with connecting rooms.
- To instruct a lock to allow a LockLink to open it – for security purposes, the LockLink must contain instructions from the Vision system that enable it to open a specific lock. The lock will not open until it receives this information.
- To change the date and time stored within a lock – each lock has a built-in clock that tracks the date and time.

Also, keycards made from the Special Keycards module, can be used to give the locks additional information. For example, a Passage-mode keycard tells the lock to remain unlocked when a valid keycard is inserted.

What the LockLink module does

The Vision LockLink module transfers lock programs and data **from** the Vision system to the LockLink.

Lock Event information can be transmitted from the LockLink **to** the Vision system. This is handled directly within the Vision Reports module, enabling reports to be viewed

immediately after the events are received. *In earlier versions of Vision the LockLink module received the events and then the Reports module had to be run in order to view them.*

NOTE: The following section gives instructions on using the LockLink module, but does include full information on using the LockLink itself. For that, you need to refer to Chapter 4 of the manual.
--

Quick Steps to using the LockLink module

Task	Beginning from the Lock Link menu screen:
Loading the LockLink with data to program locks	<ul style="list-style-type: none">• Touch Program Locks• Check that the LockLink is connected to the workstation using ActiveSync.• Enter or select (by Lock or by Group) one or more room numbers into the Selected locks list.• Touch the Send button
Loading the LockLink with data to open locks	<ul style="list-style-type: none">• Touch Open Lock• Check that the LockLink is connected to the workstation using ActiveSync.• Enter or select (by Lock or by Group) one or more room numbers into the Selected locks list.• Touch the Send button

How to load the LockLink with data to program locks

Program Locks

Send Help Logout Back

Selected locks

501 - 510

601 - 610

Add Remove

Enter by Lock by Group

Lock (s)

7 8 9

4 5 6

1 2 3

0 BkSpc

20 locks selected. 11:58:49 18/09/2002

1. Use System Setup module to establish or change your lock groups, keycard types and user groups.
2. Connect the LockLink to the workstation using Microsoft ActiveSync. *See Chapter 4 of the manual for more details on setting up ActiveSync.*

TIP: *The Vision LockLink software does not have to be running on the LockLink Pocket PC. You can start it after transferring data.*
3. If the **Main** menu of the LockLink Module is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **LockLink**.
4. Touch **Program Locks**.
5. Now select rooms you wish to program to the '**Selected Locks**' list. There are three ways to select the rooms :
 - With the **Enter** tab selected, use the keypad to enter the room number or range of room numbers for the lock(s) you wish to program.
 - OR
 - With the **by Lock** tab selected, choose room numbers from the list
 - OR
 - With the **by Group** tab selected, choose one or more entire lock groups

TIP: Choosing whether to use the *Enter* tab, the *by Lock* or the *by Group* tab:

Using the **Enter** tab is faster for blocks of rooms. You only need to enter the first and last numbers into the two small windows.

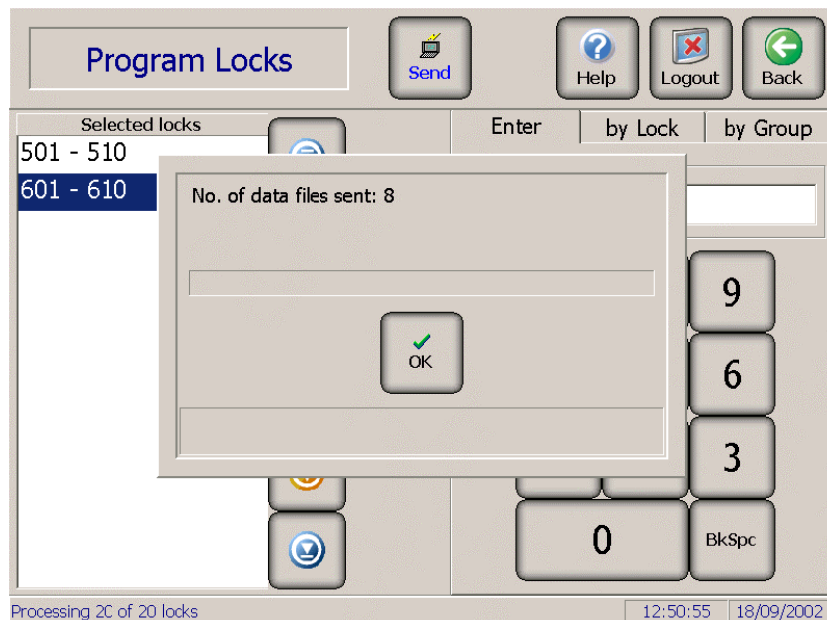
Using the **by Lock** tab is great for reprogramming a single lock or if for any reason, you want to see the list of room numbers.

Using the **by Group** tab is convenient for programming a group of locks.

6. Whichever selection method you used, move your selections to the '**Selected Locks**' list using the **add** button. If you make a mistake, you can use the **remove** button to undo it.

TIP: If you have suites or connecting rooms: Do not be concerned with connecting rooms or suites when choosing room numbers. Just program each lock, and the Vision system will automatically set up the connecting rooms correctly.

7. Touch the **Send** button. The necessary data will be transferred to LockLink. Follow any on screen instructions and press **OK** to finish the process.



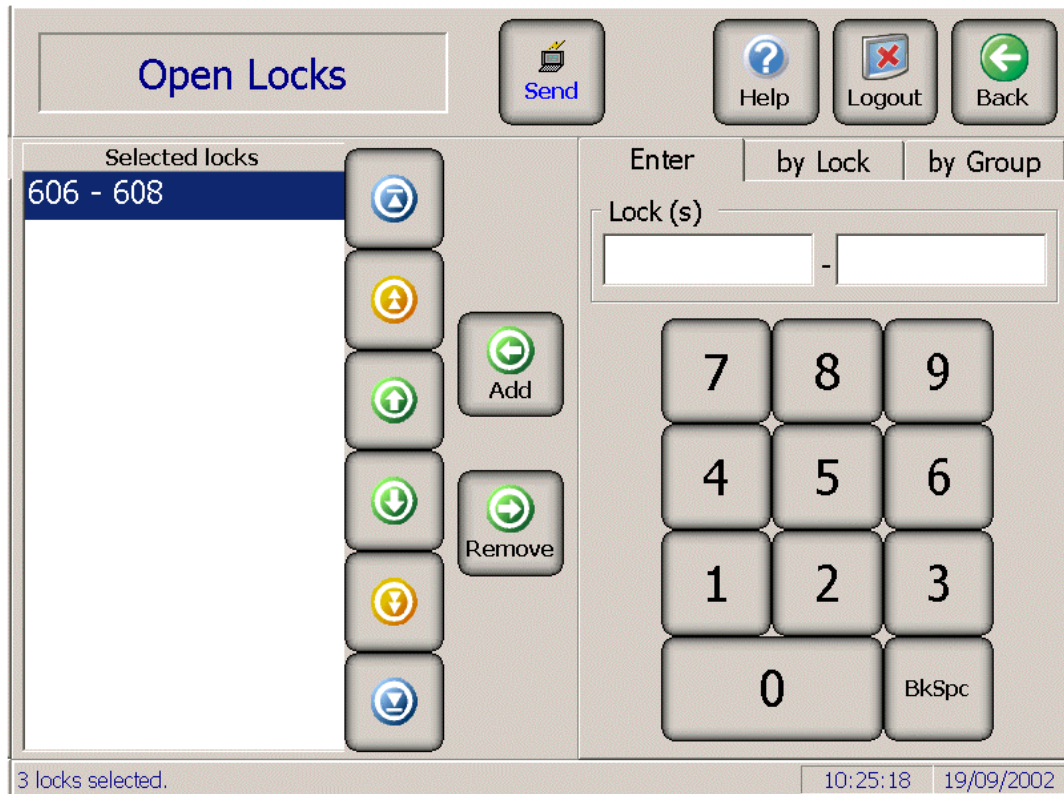
Unlocking Doors with LockLink

About Opening Locks with a LockLink

The LockLink can be used to open any lock. Normally, this is only done if the battery within the lock is too weak to open it or in an emergency situation.

Before a lock can be opened with the LockLink, it needs to receive special 'Open door' data from the LockLink module. You can authorize LockLink to open up to 10 locks. The authorization lasts 1 hour. These measures are taken for security purposes, so that the LockLink cannot open doors without proper authorization.

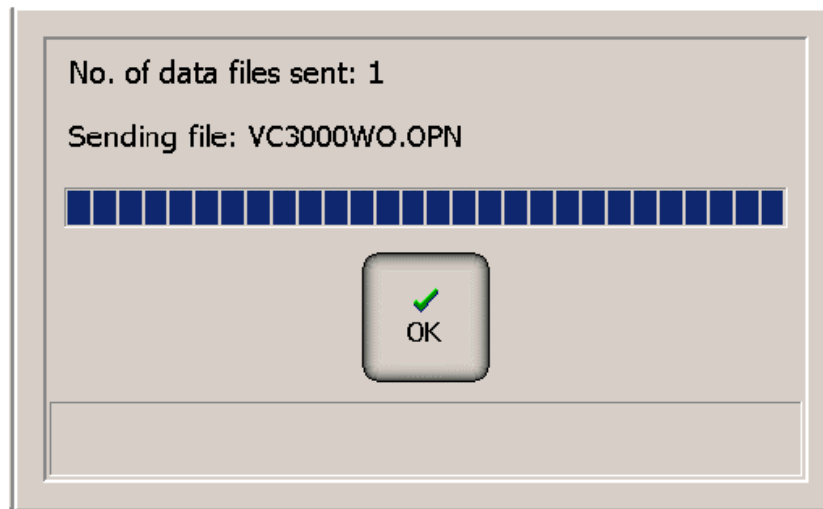
How to load the LockLink with data to open locks



1. Use System Setup module to establish or change your lock groups, keycard types and user groups.
2. Connect the LockLink to the workstation using Microsoft ActiveSync. See Chapter 4 of the manual for more details on setting up ActiveSync.
TIP: The Vision LockLink software does not have to be running on the LockLink Pocket PC. You can start it after transferring data.
3. If the **Main** menu of the LockLink Module is not displayed, touch the **Back** button to return to the Vision **Main** menu, and then select **LockLink**.
4. Touch **Open lock**
5. Now select rooms you wish to unlock to the '**Selected Locks**' list. There are three ways to select the rooms :
 - With the **Enter** tab selected, use the keypad to enter the room number or range of room numbers for the lock(s) you wish to program.
OR
 - With the **by Lock** tab selected, choose room numbers from the list
OR
 - With the **by Group** tab selected, choose one or more entire lock groups

TIP: *Choosing whether to use the Enter tab, the by Lock or the by Group tab:*
*Using the **Enter** tab is faster for blocks of rooms. You only need to enter the first and last numbers into the two small windows.*
*Using the **by Lock** tab is great for choosing a single lock or if for any reason, you want to see the list of room numbers.*
*Using the **by Group** tab is convenient for choosing a group of locks.*

6. Whichever selection method you used, move your selections to the '**Selected Locks**' list using the **add** button. If you make a mistake, you can use the **remove** button to undo it.
7. Touch the **Send** button. The necessary data will be transferred to LockLink. Follow any on screen instructions and press **OK** to finish the process.



Reports Module



Reports

Preview

Help

Logout

Back

System events

Lock

Employees

Setup

Entry Log

From date: time:

Until date: time:

Find:

☒ Room
☐ System user
☐ Keycards events
☐ All events

Fri	Sat	Sun	Mon	Tue	Wed	Thu
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

◀

October 2002

▶

© Copyright 2002 by VingCard
08:07:19 11/10/2002

What the Reports Module Does

Generates all necessary reports relating to the Vision system and the Hotel Locks. All reports can be viewed on screen, printed to a printer and saved as .txt or .rtf files if required.

The following types of reports can be generated:

- **System Events Reports** – Includes the dates and times of who logged in and what they did while logged in. You can also request a report on a specific room or user.
- **Lock Events Reports** – After downloading lock interrogation information from a LockLink or a Smart Card to a PC, you can generate a Lock Events Report.
- **Employees Reports** – Contains the information for all employees that were added from the System Users or Employee Keycards modules.
- **Setup Reports** – Detailing various setup information.
- **Entry Log** – Allows a Smart Card to be read and a report compiled to show which doors it has opened – and when.

How to Preview, Print and Save Reports

Whichever report you choose, the steps required to Preview, Print and Save the information are the same.

1. Once you have selected the type of Report you want and the set any required parameters (for example Room Name for a system event or a lock event report), Press **Preview**.



2. The Report will be shown on screen.
NOTE : *In order to view, print or save a report, the PC you are working on must have a default printer set up. You can access printer settings via the Windows Start Button. Consult you system administrator if necessary.*
3. There are 3 ways to navigate through the report.
 If you touch / click on the report (white area) or tab to it, you can use the **keyboard** arrows, Page Up, Page Down , Home and End keys to navigate the current page.
 - Home : Top of page
 - End : Bottom of page
 - Page Up : Up a third of a page (about a screen full)
 - Page Down : Down a third of a page (about a screen full)
 - Up Arrow : Up a line
 - Down arrow : Down a line

Alternatively, you can use the **on screen navigation bar**.



The buttons work as follows, from left to right :

- Start of Report
- Top of previous page
- Up / back a third of a page (about a screen full)
- Down / forward a third of a page (about a screen full)
- Top of next page
- End of Report

Finally, you can **click** (or touch for touchscreens) on the report :

- click near bottom of report to scroll down
- click near top of report to scroll up

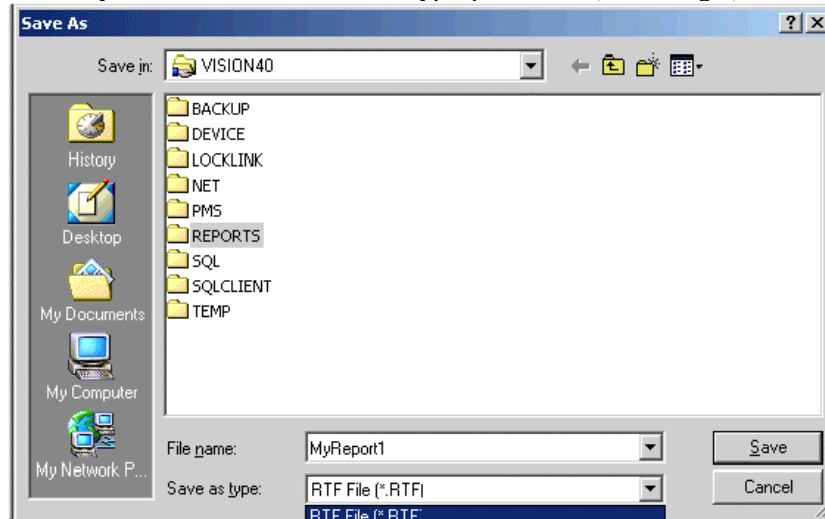
4. To print the report on your PC's default printer, press **Print**.



NOTE : *Be sure to wait until the report preview is complete before printing or saving. This can be observed by looking at the status message in the*

bottom left corner of the screen

5. To Save the report press **Save**. A 'Save As' screen will appear which allows you to select a file name and browse to the location you wish to save to. You can save the report either as a plain text file (.txt) or as a Rich Text Format (RTF) file. RTF files can be read by all major word processors will look very similar to the on screen report when later viewed or printed. When you have selected your location, File name and type, press Save (bottom right).



Available System Reports

System Events Reports

The Vision system stores information such as who used the system and what they did while they were logged in. The System Events Reports allow you to view or print this information.

You choose start and end dates of reports. If you do not want to include all event information in the report, you can choose to generate a report for just a specific Room number or a particular User.

How to Run System Events Reports

Reports

Preview Help Logout Back

System events Lock Employees Setup Entry Log

From date: 11/10/2002 time: 00:00

Until date: 11/10/2002 time: 08:23

Find:

☐ Room

☒ System user

☐ Keycards events

☐ All events

names	Id
Mellie, Roger	f100
VingCard, Demo1	VingCard 1
VingCard, Demo2	VingCard 2
Welsh, Trevor	W345

© Copyright 2002 by VingCard 08:22:48 11/10/2002

1. Select the **System Events** tab
2. Set the date and time limits for the report – all events between the **From date : time** and the **Until Date : time** will be displayed.

To set dates, touch the displayed from or until date and then select the required date from the calendar that appears on the right side of the screen.

To set times, touch the displayed from or until time and then select the required time from the clock that appears on the right side of the screen.

Whether the clock is in am/pm or 24 hour mode is dependent on your PCs Windows 'Regional Settings'.

If the AM and PM buttons appear under the clock, you can touch either of them to switch between AM and PM.

OR

If the 1-12 and 13-24 buttons appear under the clock, you can touch either of them to switch between the first and last 12 hours of the day.

3. Touch the check box in front of one of the following:
 - Room** – choose from the room numbers on the right side of the screen.
 - System User** – choose a user from the list on the right side of the screen
 - Keycard events** – choose a card holder from the guest or employee list on the right side of the screen. The lists include all keycards that have been verified. All events relevant to the cardholder will be shown.
 - All events** – no need to make any other selections for this report.

NOTE: *Some hotels are setup to allow guests to be check into connecting rooms or suites. During Check In, you select a room number and then use the Connecting Rooms button to select from the connecting rooms list.*

When making a report for a suite, you should enter the room number you entered at check in time (before selecting the Connecting rooms button). If you enter one of the other room numbers of the suite, no events will be reported for them.

On the report itself, you can differentiate between events affecting suites and those affecting single rooms by looking at the 'Keycard Type' field.

4. When you have finished making selections from this screen, touch the **Preview** button.

Employees Reports

These reports show the Names and Employee ID for all employees. If an employee has been assigned a keycard, the card's User Group, unique User Id and start and expiration dates will be shown. If an employee has been given access to any Vision system modules, their System Access Group will be displayed.

All employee information currently in the database is always included in the report, but you can sort it based on any of the following:

- (Employee) Name
- (Employee) ID
- User Group
- System Access Group

For security purposes, password (and login username if applicable) is NOT included in employee reports.

How to Run Employees Reports

Reports

Preview Help Logout Back

System events Lock Employees Setup Entry Log

Sort by :

☐ Name

☐ ID

☐ User group

☒ System access group

© Copyright 2002 by VingCard 09:04:13 11/10/2002

1. Select the **Employees** tab
2. Touch the check box in front of one of the following:
Name – to sort the report by Name
ID – to sort the report by Employee Id
User Group – to sort the report by keycard user group
System Access Group – to sort the report by System Access Group
3. When you have made your selection from this screen, touch the **Preview** button.

Setup Reports

These reports show various aspects of the system setup. There is a separate report for the following :

- Common Door Information
- Keycard Type Interrelation information
- Lock Types information

How to Run Setup Reports

The screenshot shows the 'Reports' screen in the VingCard Vision 4.1 software. At the top, there is a 'Reports' button and three icons: 'Preview', 'Help', 'Logout', and 'Back'. Below these are tabs for 'System events', 'Lock', 'Employees', 'Setup', and 'Entry Log'. The 'Setup' tab is currently selected. In the 'Report:' section, there are three checkboxes: 'Common doors' (checked), 'Keycard Interrelations' (unchecked), and 'Lock Types' (unchecked). The bottom of the screen displays the copyright notice '© Copyright 2002 by VingCard' and a timestamp '09:13:21 11/10/2002'.

1. Select the **Setup** tab
2. Touch the check box in front of one of the following:
Common Doors – to list out all defined Common Doors
Keycard Interrelations – to show a matrix of which keycard types interrelate to each others. That is, which keycard types will invalidate which others when used in locks.
Lock Types – to show a list of all available VingCard lock types and which rooms are allocated to each lock type. Also shown is which card family type (mag-stripe, Smart Card etc) each lock type accepts
3. When you have made your selection from this screen, touch the **Preview** button.

Available Lock Reports

Lock Events Reports via LockLink

The LockLink Pocket PC can be used to read Lock Event information from each lock and transfer it to a Vision PC. This data can be viewed or printed as a Lock Events Report.

Lock Event Reports show all events related to use of the lock, including a full record of exactly who entered the room and when.

VingCard locks can store up to 100 or 200 lock events – dependent on lock type. The VC3000 Classic locks store up to 100 events, DaVinci and Presidio up to 200.

NOTE : Lock event reports can often be used to help staff wrongly accused of something by guests.

For full details on how to use LockLink to extract Lock Events, see Chapter 4 of this manual.

How to Run Lock Events Reports via LockLink

The screenshot displays the 'Reports' section of the VingCard Vision 4.1 software. The interface includes a top navigation bar with buttons for 'Reports', 'Preview', 'Help', 'Logout', and 'Back'. Below this is a tabbed menu with 'System events', 'Lock', 'Employees', 'Setup', and 'Entry Log'. The 'Lock' tab is active, showing a sub-menu with 'LockLink', 'Readout card', and 'Service Card'. The 'LockLink' sub-menu is selected, displaying a table of lock events. To the right of the table are buttons for 'Receive' and 'Delete'. At the bottom, there is a status bar showing the copyright notice '© Copyright 2002 by VingCard', the time '09:21:43', and the date '11/10/2002'.

Lock events	Date	Time
501	08/10/2002	09:47
1001	06/08/2002	10:36
606	27/10/2002	02:04
607	19/09/2002	10:07
c1	30/09/2002	10:53
c3	30/09/2002	10:35

1. Select the **Lock** tab and then the **LockLink** sub-tab
2. If you just want to re-view previously downloaded events, go to step 4 . To download new events :

Press **Receive**. A pop up screen will appear. Press **Start** when the PC and LockLink are connected via Microsoft ActiveSync.

NOTE : *See Chapter 4 of the manual for more details on setting up ActiveSync.*

3. The lock events will be transferred to your PC. The on-screen room list will be updated with all the events from the LockLink.

NOTE: *The list will be completely replaced with the new data received from LockLink. However, unless previous events are deleted from the LockLink device they will actually be recopied to the PC. Example : LockLink reads events for Room 100 and transfers to PC. PC list shows Room 100. Days later, LockLink reads events for Room 200. LockLink now contains data for Room 100 and 200. When events are transferred to PC, PC list shows 100 and 200. If Room 100 events had been removed from the LockLink, then after transfer of Room 200 events, Room 100 Events would not be available from the PC either.*

4. Select a room from the list and press **Preview**
5. To remove the events for a given room from the list, select the room on the list and press **Delete**

NOTE: *As indicated above, this will only remove record of those lock events from the PC. They may still be available if you re transfer from the locklink.*

*If you need a permanent copy of events for a room, then Preview and **Save** a report.*

Only delete lock events from the LockLink if you are sure you will not need them again.

Lock Events Reports via Readout Card

A Readout Card can be used to read Lock Event information from locks that accept Smart Cards and transfer it to a Vision PC. This data can be viewed or printed as a Lock Events Report.

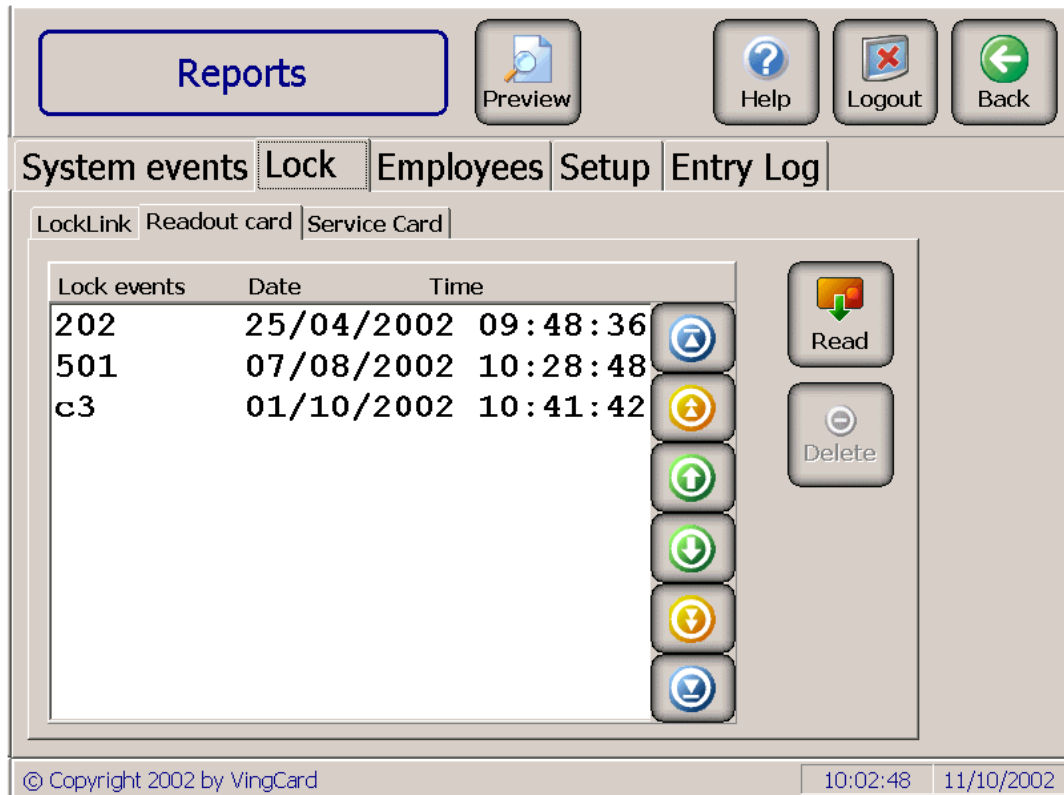
Lock Event Reports show all events related to use of the lock, including a full record of exactly who entered the room and when.

VingCard locks can store up to 200 lock events – dependent on lock type and manufacture date.

<p>NOTE : Lock event reports can often be used to help staff wrongly accused of something by guests.</p>

A Readout card is a special type of Smart Card. See the Special Cards section of this chapter for details.

How to Run Lock Events Reports via Readout Card



1. Select the **Lock** tab and then the **Readout card** sub-tab
2. If you just want to re-view previously downloaded events, go to step 4. To download new events :
Press **Read** and insert a Readout Card into your Smart Card reader. Remove the card when prompted.
3. The lock events will be transferred to your PC from the Smart Card. The on-screen room list will be updated with the events from the card.

NOTE: The list will be added to by the new data received. Older versions of Events for the same room will be replaced.

4. Select a room from the list and press **Preview**
5. To remove the events for a given room from the list, select the room on the list and press **Delete**

NOTE: This will remove record of those lock events from the PC. Unless they are still retained on the Readout Card they will in effect be permanently deleted.

If you need a permanent copy of events for a room, then **Preview** and **Save a report**.

Only delete lock events from the Readout Card list if you are sure you will not need them again.

Lock Service Data Reports via Service Card

A Service Card can be used to read Lock Service information from locks that accept Smart Cards and transfer it to a Vision PC. This data can be viewed or printed as a Report.

Lock Service information contains data of interest to lock maintainers : battery level, failure rate for the card reader in the lock etc.

A Service card is a special type of Smart Card. See the Special Cards section of this chapter for details.

How to Run Lock Service Data Reports via Service Card

The screenshot shows the 'Reports' section of the VingCard Vision 4.1 software. The 'Lock' tab is selected, and the 'Service Card' sub-tab is active. The 'Service Card' section contains the following fields:

Room:	<input type="text"/>
Lock type:	<input type="text"/>
Lock mode:	<input type="text"/>
Battery:	<input type="text"/>
Cylinder:	<input type="text"/>
Smart card	Magnetic card
Openings:	<input type="text"/>
Insertions:	<input type="text"/>
Misreads:	<input type="text"/>

A 'Read' button is located to the right of the 'Service Card' section. The 'Preview' button is located at the top right of the 'Reports' section. The bottom status bar shows the copyright notice '© Copyright 2002 by VingCard' and the date and time '10:30:51 11/10/2002'.

1. Select the **Lock** tab and then the **Service card** sub-tab
2. Press Read and insert a Service Card into your Smart Card reader. Remove the card when prompted.
3. The lock service data will be transferred to your PC from the Smart Card
4. Read the on screen data. Press Preview if you want to print or save a report.

Entry Log Reports via Guest or Employee Smart Cards

A Smart Card can be read to show a history of what rooms it has been used to enter. This data can be viewed or printed as a Report.

For this to work, the User Group for the Smart Card in question must have been set up with the 'Entry Log' option checked.

A Smart Card can hold up to 400 individual entry records.

How to Run Entry Log Reports via Guest or Employee Smart Cards

The screenshot displays the 'Reports' section of the VingCard Vision 4.1 software. At the top, there is a 'Reports' button and a 'Preview' button. To the right are 'Help', 'Logout', and 'Back' buttons. Below these is a navigation bar with tabs for 'System events', 'Lock', 'Employees', 'Setup', and 'Entry Log'. The 'Entry Log' tab is currently selected. The main area is divided into two panels. The left panel, titled 'Guest', contains fields for 'Room:' (100), 'Keycard type:' (Single Room), 'First name:', 'Last name:', 'User group:' (V.I.P Guest), 'Valid from:' (11/10/2002 09:3), and 'Valid until:' (13/10/2002 14:0). The right panel, titled 'Smart card information', displays the message 'Guest card is read. Found 1 entry records' and a 'Read' button with a green arrow icon. At the bottom of the window, the copyright notice '© Copyright 2002 by VingCard' is on the left, and the time '10:40:38' and date '11/10/2002' are on the right.

1. Select the **Entry Log** tab
2. Press Read and inset the guest or employee Smart Card into your Smart Card reader. Remove the card when prompted.
3. The Entry Log data will be transferred to your PC from the Smart Card
4. Read the on screen data. Press Preview if you want to view, print or save a more detailed report showing all rooms entered with date and time.

NOTE : *The Entry Log does not contain a record of locks where the card was inserted but did not unlock the door. This is for security purposes – so that an Entry Log cannot be manipulated to contain ONLY failed (or false) attempts to open doors, thus masking the record of doors actually unlocked.*

Glossary of Terms

Check Out Date and Time – All guest keycards contain the date and time of check out. This information is stored on the keycard so that the locks will know when the keycard expires.

Common Doors – When you make a guest keycard, you can give access to doors (such as car parks or pool areas) in addition to the bedroom. These are called Common Doors. Guest access to Common Doors ends when the keycard expires (not when a newer guest keycard is used on the lock.)

Contact Card – The black plastic card that is attached to the LockLink. It is inserted into locks to program or interrogate them.

Deadbolt Override – Available depending on your hotel's setup. Allows a keycard to open a lock, even if the deadbolt has been set. For guest keycards, this can be assigned when the keycard is made. For employee keycards, this is determined solely by the User Group.

Employee ID – Whenever you add an employee to the System User or Employee Keycards module, you will be required to assign a unique Employee ID. The same ID is used for both modules. This is not the same as employee Username Passwords.

Events – see either Lock Events or System Events

Fail-safe Keycard – Fail-safe keycards are pre-made keycards, created so that if the computer ever goes down, guests can still be checked in. They work in conjunction with Programming keycards. There are two kinds of Fail-safe keycards; see Sequential Keycards and Random Keycard. See Special cards section for more information.

Future Proof™ – VingCard systems are created using the latest technology and are carefully designed with the future in mind. We are so sure of this, that we trademarked the term FutureProof!

Interrogating a Lock – Up to 100 lock events can be "read" from VC3000 Classic lock, or up to 200 events from DaVinci / Presidio lock by a LockLink. This is sometimes called interrogating a lock.

Issue area – Normally, the entire hotel will have the same Issue area (the front desk). Each hotel has the option of assigning additional Issue areas in the System Setup module.

Lock Events - Anything that happened to a lock, such as having a keycard or metal key used in it are called Lock Events. The LockLink module allows you to download this information from the locks and then the Reports module allows you to generate a Lock Event report. You can optionally include Lock Events when you Backup.

LockLink – A hand-held computer whose main function is to transfer data between the computer system containing the Vision system (LockLink module) and the locks. It can also Interrogate or open locks.

Lock-out Keycard – Lock-out keycards are not used by all hotels. They prevent a guest from returning to a room between the time they check out and the time their keycard expires.

Passwords – Unique number assigned to each employee. It must be entered by the employee on the Log-in screen and is used to identify the user to the Vision system.

Programming keycard – the Programming keycard is used on a lock prior to a Fail-safe keycard. It tells the lock to allow a Fail-safe keycard to work.

Programming locks – Each hotel can reprogram locks by making changes on a computer with the Vision system on it, and then transferring the data to the locks. A LockLink is used for this transfer.

Property Management System Interface (PMS) – Your hotel may have property management software that sends and receives information to and from the VingCard software. The ability to transfer information this way is called interfacing.

Random Fail-safe Keycards – Method of creating Fail-safe keycards that can be used for ANY door. When the guest checks in, you will need to use a Fail-safe Programming keycard and then a Fail-safe keycard on the door before giving the Fail-safe keycard to a guest.

Sequential Fail-safe Keycards – Method of using Fail-safe keycards that lets you create up to 8 Fail-safe keycards for each SPECIFIC door. This method results in Fail-safe keycards that are completely ready to give to guests if the computer system ever goes down.

Special keycard – Any keycards made from the Special Cards module of the Vision system.

System Access – The Vision system consists of several modules. Your hotel uses the System Users module to determine access to each.

System Events – The Vision system keeps track of information, such as who accessed the system and what they did. The Reports module allows you to generate a System Events report and Backups can optionally include System Events.

Toggle Mode keycard – These keycards do not actually open a lock, but are used to temporarily tell a lock to remain unlocked the next time it is opened. Normally used for banquet rooms, or rooms you want to give people access to who do not have a keycard.

User Group – Every guest and employee keycard is assigned to a User Group to control access. User Groups include; User Type (see Setup module for details), which doors to unlock, and whether the keycard has deadbolt override authority.

User ID – Every guest keycard is assigned a User ID by the Vision system when it is made. This number can be used to identify it in the future. This is not the same as an Employee ID.

Frequently Asked Questions

1. What if a guest's keycard does not work?

Answer: If a mag-stripe keycard is exposed to magnets, it will be erased and you will need to remake it. To determine if the keycard was made for the correct room, you can use the Verify option in the Guest Keycards module.

2. What is the difference between making Duplicate guest keycards and Replacing a lost or stolen guest keycard?

Answer: A *replaced* keycard will invalidate original guest keycard, so that lost or stolen keycard will no longer open the door to the room. For security reasons, a keycard that is lost or stolen **MUST** be replaced rather than duplicated. If there are roommate cards, they will **NOT** need to be replaced.

Making a *duplicate* keycard will not invalidate older keycards. Normally, they are used to allow a roommate to have their own keycard.

3. Why won't Verify show me the information on a keycard?

Answer: When you use Verify, a blank keycard, a keycard made from a different module, a keycard from a different hotel, or a damaged keycard will result in an error message.

4. Does the Vision system know whose keycard opened a specific door?

Answer: Yes. The lock can be "read" using a LockLink or a readout card and the results can be transferred to the Vision system.

5. Does the Vision system know who made a keycard?

Answer: Yes, the System Events Reports include this information.

6. When is it necessary to use the Check Out option of the Guest Keycards module?

Answer: Many hotels do not use this option, but your hotel may need to use it to interface with a Property Management System. Check with your Vision system administrator.

7. Is there anything I need to know about the care of keycards?

Answer: Keycards are vulnerable to the same damage as credit cards. They will not function if exposed to magnets or extreme heat. Eel skin and many other types of leather used in wallets can erase keycards.

8. Is there anything special I need to know about the Vision Touch Screen?

Answer: The surface of the screen is glass and was designed to be touched with your fingers. Do not use anything abrasive, such as a pencil eraser to make selections. It can

be cleaned like any other computer screen.

- 9. Is there a way to open a door if the batteries in a lock become too low to open the lock?**

Answer: Yes, this is one of the functions of the LockLink.

Chapter 6 : PMS Interface

About Interfacing Vision with a PMS

VingCard Vision provides three standardised interface methods by which a Property Management System (PMS) can control the issue and maintenance of guest keycards.

These are :

- **TCP/IP Interface**
This is the most powerful and flexible integration method available, allowing access to guest keycard functionality from any PMS workstation that has TCP/IP capability – regardless of physical location.
- **Direct Integration via DLL calls**
This is a powerful and flexible integration method in which VingCard makes available a Windows 32 bit DLL which exports functions related to the issue and maintenance of guest keycards. The PMS software loads the DLL is then able to use the library of DLL functions.
- **RS232 Serial connection**
Using a standard RS232 serial link and through by use of the defined message protocol, the PMS is able to issue commands to encode and verify keycards on the VingCard system.

How to use the PMS system

There are many different PMS systems, each with it's own specific user interface. Please refer to the User Manual for the PMS system that your Hotel / Ship uses.

Where to find detailed information on the Vision PMS interfaces

VingCard has produced a comprehensive Software Developers kit to enable PMS to Vision interfaces to be rapidly and accurately developed.

For each interface method, the SDK provides detailed **usage** and **protocol descriptions**, along with working code samples written in Visual C++, Borland Delphi and Visual Basic.

The aim is to provide sufficient information to allow efficient and error free programming of the PMS side of the interface.

If you require a copy of the PMS SDK, please contact your VingCard dealer.

Specific PMS issues in 'mixed card' properties

A mixed card property in this case is one that uses both mag-stripe and Smart Cards.

Making keycards

When making, changing or replacing guest cards, Vision examines the User Group sent in the PMS request to determine whether it needs to make a mag-stripe or a Smart Card.

It then checks the destination address sent by the PMS. There are 4 possibilities :

- the address maps to one network encoder as defined in the **Vision Setup > System Parameters > PMS RS232 > Address Mapping table**. The network encoder is of the correct type for the user group (i.e. Smart or mag-stripe). A card will be made.
- the address maps to one network encoder as defined in the **Vision Setup > System Parameters > PMS RS232 > Address Mapping table**. The network encoder is of the wrong type for the user group (i.e. Smart or mag-stripe). A card will NOT be made. An error code will be sent to the PMS. The code will be '1' (Unspecified Error) if the option 'Extended PMS error codes' is not checked in **Vision Setup > System Parameters > Smart Card Options** or '14' (hexadecimal E – Incompatible card type) if the option is checked. *You should leave the option unchecked unless your PMS has been updated to recognise the new error code.*
- the address maps to two network encoders (one mag, one smart) as defined in the **Vision Setup > System Parameters > PMS RS232 > Address Mapping table**. The network encoder of the correct type is chosen and a card will be made.
- the address maps to a Vision PC as defined in the **Vision Setup > System Parameters > PMS RS232 > Address Mapping table**. The local encoder of the correct type is chosen and a card will be made. *Local encoder = those mapped using the Vision Setup > System Parameters > mag card encoder and >smart card encoder screens.*

The basic philosophy here is that existing PMS interfaces do not have to change. The PMS sends the same address and user group as it previously has and the Vision system makes the correct card. The only changes to go from a one card type to a two card type system are

- the addition of a Smart Card encoder at appropriate check in locations and
- (if network encoders are used) the double mapping of a single PMS address to two physically adjacent encoders (one mag, one smart) in **Vision Setup > System Parameters > PMS RS232 > Address Mapping table**.

Verifying keycards

When the PMS sends a verify command to Vision, there is no additional information (such as user group) that allows Vision to determine whether a Smart or mag-stripe card should be verified. The only information sent is the destination address.

Therefore, to verify keycards via the PMS, the destination address must map specifically to a single network encoder in **Vision Setup > System Parameters > PMS RS232 > Address Mapping table**. In this case, Vision will prompt for a card to be inserted in that specific encoder. *If you have two network encoders at one location – one Smart and one mag - and you wish to use the PMS verify command, then you can make sure that each encoder has a separate address. However, this means that the PMS side of the interface needs to 'know' about a new address.*

If the destination address maps to 2 network encoders (one Smart, one mag) then an error ('1') will be returned.

If the destination address maps to a Vision PC, then an error ('1') will be returned unless Vision is set into 'Full Integration Mode' (**Vision Setup > System Parameters > PMS RS232 > Integration Mode**). In this case, the user will be prompted – on the Vision PC – to choose card type.

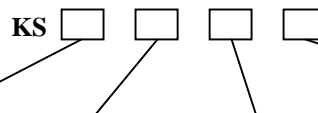
Chapter 7 : Network Encoder Setup

KDE series 493x network encoders

Hardware Overview

This encoder is a motorized insertion type magnetic stripe with RS232C and / or Ethernet interface

There are different variants of the encoder, defined by the model number, which can be interpreted as follows



Interface Type	Function	Voltage	Track or Communication Position
T Terminal	4 Read/Write	9 Customized	02 Track 3 with RS232 03 Track 1,2,3 with RS232 31 Track 3 with RS232 or Ethernet 32 Track 1,2,3 with RS232 or Ethernet

Example : KST 4903 : uses RS232 interface and can encode to tracks 1,2, & 3

DIP switch settings

The encoder needs to be correctly set up using the DIP switch on the back panel. DIP switch setting meanings are as follows :

SW1, SW2 : baud rate. (off,off=2400; on,off=4800; off,on=9600; on,on=19200)

SW3 : on = track 1 enabled ; off = track 1 disabled

SW4 : on = track 2 enabled ; off = track 2 disabled

SW5 : on = track 3 enabled ; off = track 3 disabled

SW6 : on = RS232 ; off = Ethernet (network)

Note that when using Ethernet, the baud rate switches must be set to 9600 (SW1 off, SW2 on)

Examples (SW1 to 6, 0=off, 1= on)

0,1,1,1,1,1 RS232 communication, 9600 baud, 3 track encoding

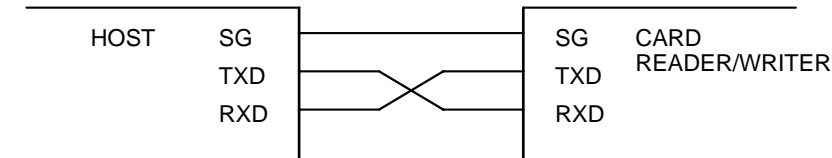
0,1,1,1,1,0 Ethernet (network) communication, 3 track encoding,

Ethernet Interface

The KDE network encoder contains a TCP/IP to RS232 protocol converter called a 'Hello Device' type HD1321. This is manufactured by Sena Technologies. Full details are available at www.sena.com. This device allows Vision to address the encoder via an Ethernet network.

RS 232 Interface

RS232 connections should be made by connecting transmit (TXD), receive (RXD) and System Ground (SG) only. A suitable cable is delivered by VingCard with the encoder if derail use is required.



When using RS232, the encoder uses 8 data bits, no parity, 1 start bit, 1 stop bit.

How to Set Up (or change) the TCP/IP Address

Overview

The IP address is set up using an Ethernet connection.

In order for Vision to be able to use the encoder, it needs to be set up with a fixed IP address. When delivered, the device has an IP address set to 0.0.0.0. When the device has power on and has IP=0.0.0.0 the device makes continual DHCP requests, requesting assignment of an IP address. The DHCP requests need to be intercepted and serviced by a PC running special encoder configuration software. This software acts as a DHCP server and provides an appropriate (user selectable) IP address back to the device. Once the device has an IP address, it keeps it, even following a power down.

It is important that when the encoder is being set up, it is isolated from any other 'external' DHCP servers on the network – for example the main DHCP server at the property. If this is not the case, then an IP address may be assigned by the external DHCP server rather than the encoder configuration software. Vision can be configured to use the assigned address, but depending on the DHCP server that originally issued it, the address may be subject to change and or re-allocation – thus leading to an unstable system.

Configuration Software

The KDE Utility configuration software needs to be installed. To do this run the file setup4kde.exe as supplied on the Vision CD. This will install the configuration software with sufficient capability to set up the encoder. The installed program is called 'HelloDevice.exe' and can be run from a desktop icon or Start > Programs > KDE_Utility

Note that there is an installation program for a fuller version of the configuration software provided on the CD, called setup_hd132x.exe. A full manual for this version of the configuration software is available from www.sena.com. However, in normal circumstances you should use the simpler software installed by setup4kde.exe.

Physical connection

The important thing is to run the configuration software on a PC that is networked to the encoder and to make sure that any connections to external DHCP servers are temporarily removed.

Example 1

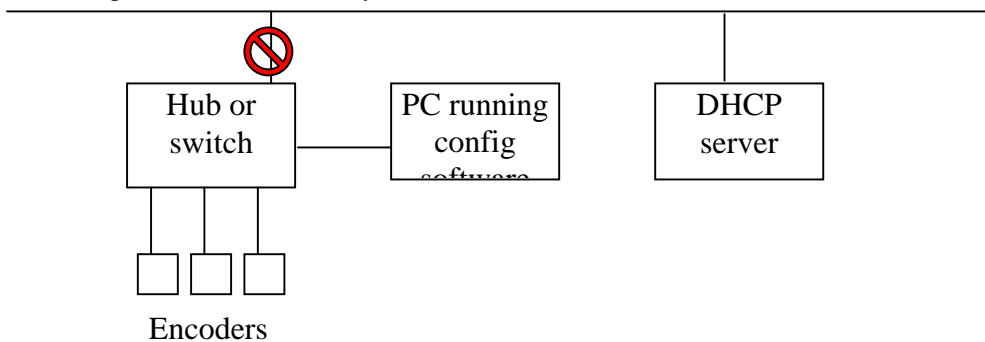
Run the software on a laptop and connect directly to the encoder using a crossover patch cable (yellow). When set up is complete, plug the encoder into its network socket.

This method is the safest as it is the least prone to ‘outside interference’ from another DHCP server and does not involve making or breaking connections at the property’s hubs and switches. However, if you have >1 encoder you need to connect to each in turn in order to set them up.

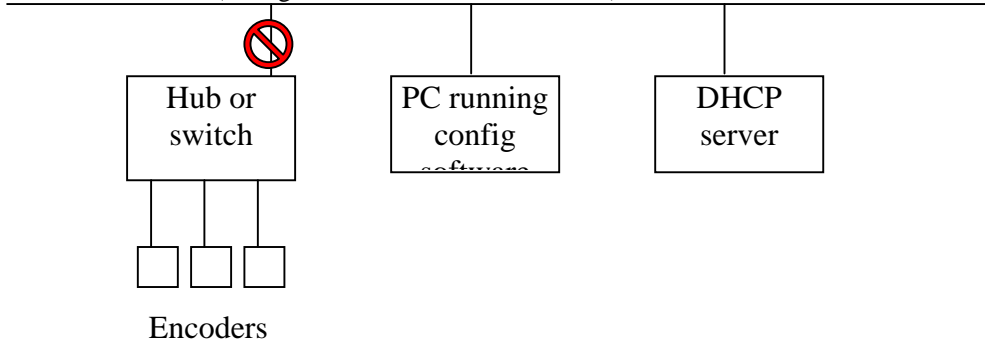
Example 2

Connect one or more encoders into their network sockets (might be directly into the property backbone, or into hubs or switches). Now break any connections between the encoders and external DHCP servers. Then run the configuration software on a PC that can communicate with all the encoders (test with PING command).

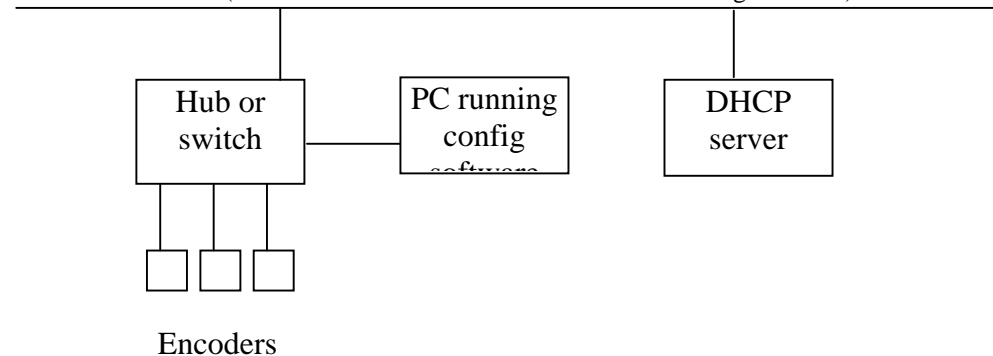
For example this would work (if you made a break as shown)



But this would not (config software cannot see encoders)



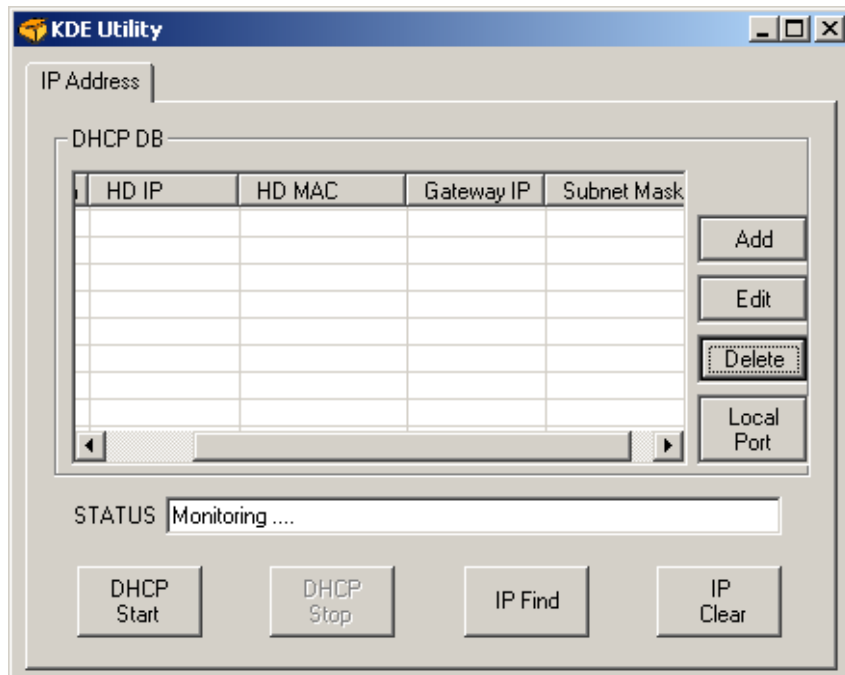
And nor would this (encoders can see DHCP server as well as config software)



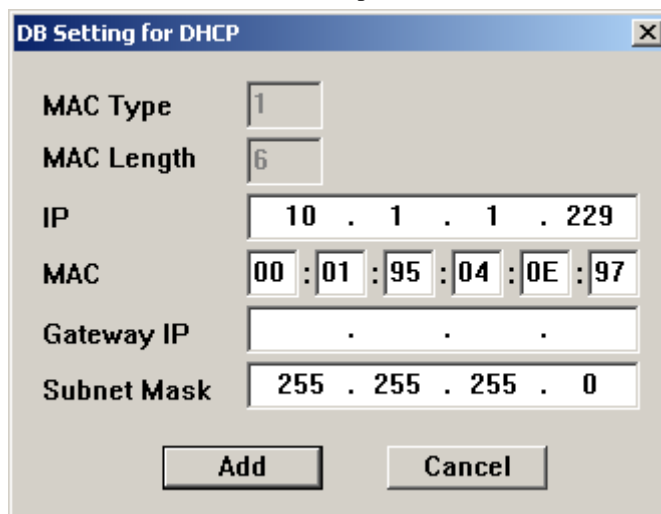
The advantage of this approach is that many encoders can be configured at once. The disadvantage is that for more complex networks with distributed encoders, it might be difficult to achieve.

Step by Step Allocation of IP Address

- 1 If it is not already installed, install configuration software ('HelloDevice.exe') on a PC by running 'Setup4KDE.exe'.
- 2 Connect the encoder(s) and a PC running the configuration software as discussed above. Leave the encoders un-powered. Check the encoder DIP switch settings are correct for Ethernet connection (1 off, 2 on , 6 off)
- 3 Launch the configuration software (by desktop icon 'KDE_Utility' or by Start > Programs > KDE_Utility. Make sure the config software DHCP server is not running. You can do this by checking the DHCP Start button is enabled.
- 4 Press the add button

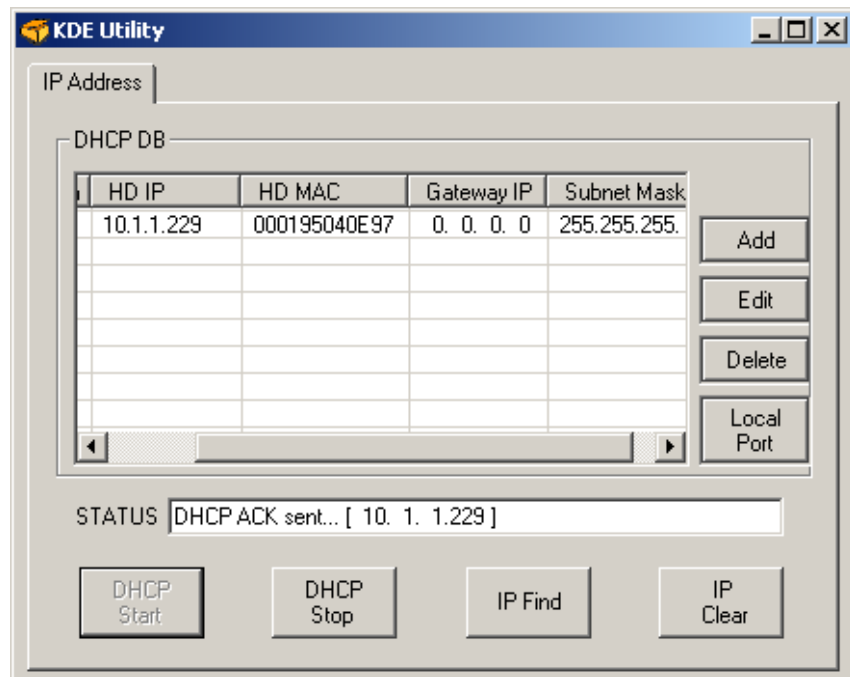


- 5 Enter the MAC address from the encoder and the IP address you wish to allocate (10.1.1.229 in this example). Press Add.

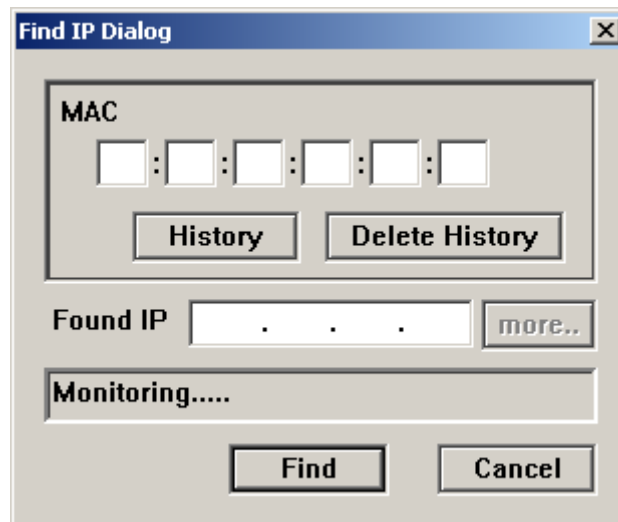


- 6 Repeat steps 2 and 3 for each connected encoder you are setting up.

- 7 Power on the encoder(s). Press DHCP Start. Each encoder, identified in the DHCP DB table (by its MAC address) should now be allocated with the correct IP. Status messages similar to that shown should be received for each.



- 8 Press DHCP Stop.
- 9 Now, for each encoder, check that the IP address has been set as expected. Press IP Find, enter the encoder MAC address (or recall it using the History button) and press Find. The IP address should match that in the DHCP DB table on the main screen.



- 10 If any encoders have not had IP address set as expected it is either because there is another DHCP server present (see section on Physical Connection) or because they already had an IP address from a previous setup – see Changing an IP address below.

Changing an IP Address

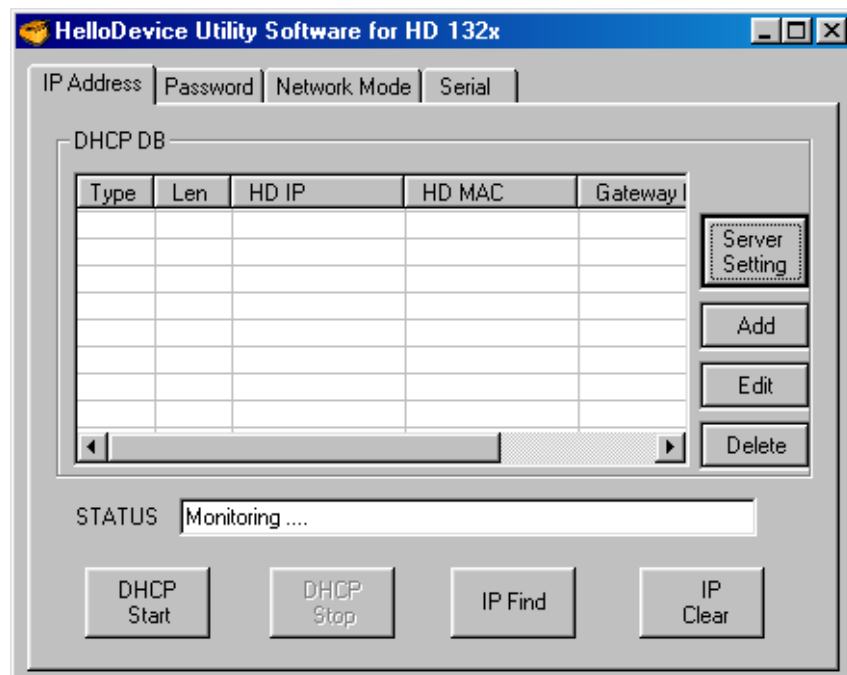
- 1 Make sure the config software DHCP server is not running. You can do this by checking the DHCP Start button is enabled.
- 2 For the encoder to be changed :
Press IP Clear, enter the correct MAC address (or recall it using the History button) and press Clear. Confirm when prompted.
The encoder now has IP address = 0.0.0.0 and will make a DHCP request.
Press DHCP Start. The IP address from the DHCP DB table will now be allocated.

Full setup Step by Step

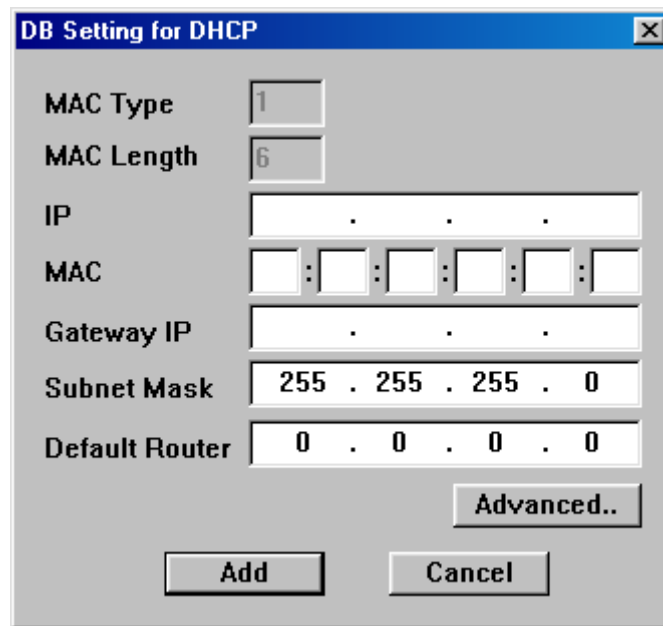
In some rare circumstances (when, not only the IP address, but also the other parameters of serial server are wrong) it will be necessary to use a full setup utility program.

Allocation of IP address (Full Setup)

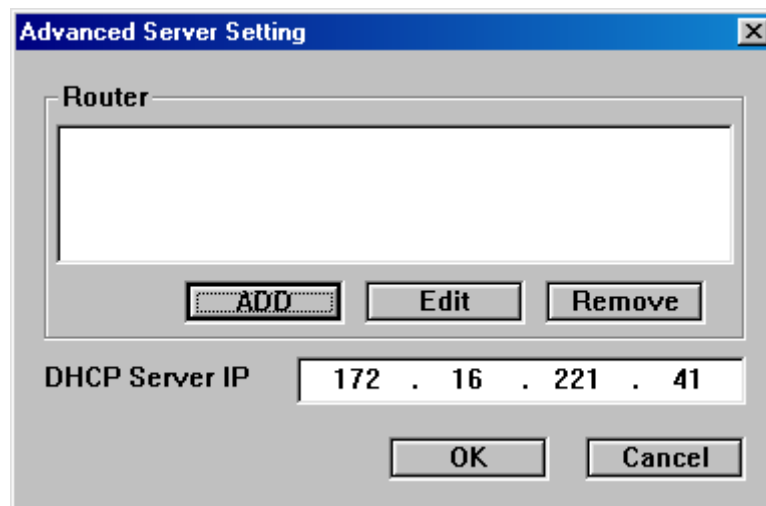
- 1 If it is not already installed, install configuration software ('HelloDevice.exe') on a PC by running 'Setup_HD132x.exe'.
- 2 Connect the encoder(s), the M200i(s) and a PC running the configuration software as discussed above in "Physical connection" paragraph.
- 3 Launch the configuration software (by desktop icon 'HelloDevice Utility Software for HD 132x' or by Start > Programs > HelloDevice Utility Software. Make sure the config software DHCP server is not running. You can do this by checking the DHCP Start button is enabled.
- 4 Press the add button



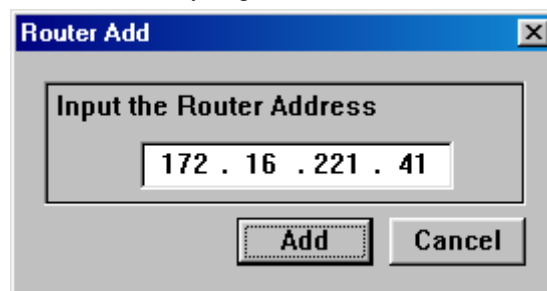
- 5 Press Advanced button.



- 6 Press ADD button

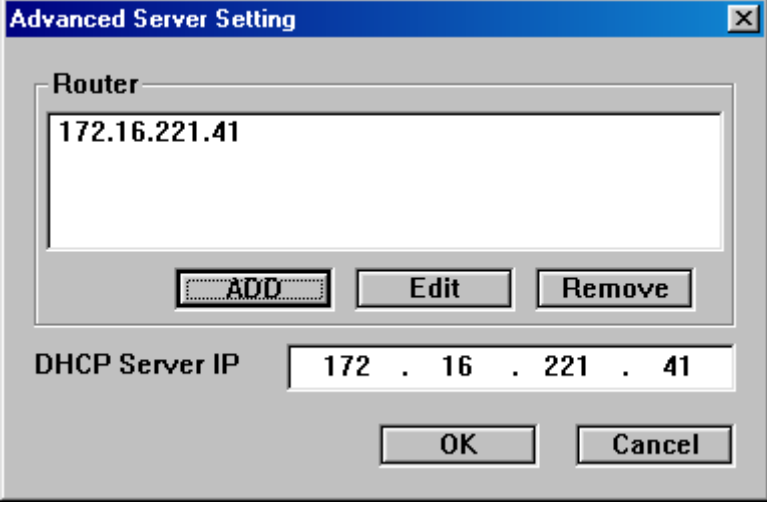


- 7 Enter the IP address of your PC, on which you work. Use WINIPCFG or IPCONFIG utility to get it, if unknown.



Click Add button.

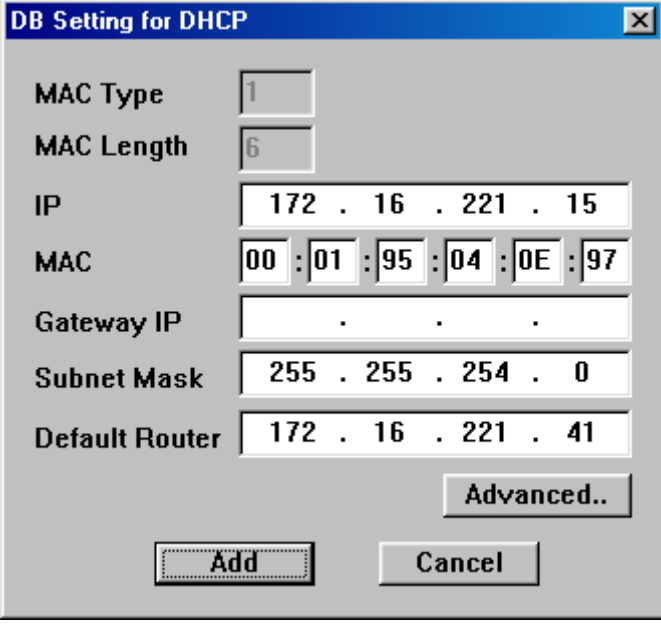
- 8 Click OK to confirm.



The 'Advanced Server Setting' dialog box has a title bar with a close button. It contains a 'Router' section with a text field displaying '172.16.221.41'. Below this field are three buttons: 'ADD', 'Edit', and 'Remove'. At the bottom, there is a 'DHCP Server IP' section with a text field showing '172 . 16 . 221 . 41' and two buttons: 'OK' and 'Cancel'.

Your PC IP address is stored as a router.

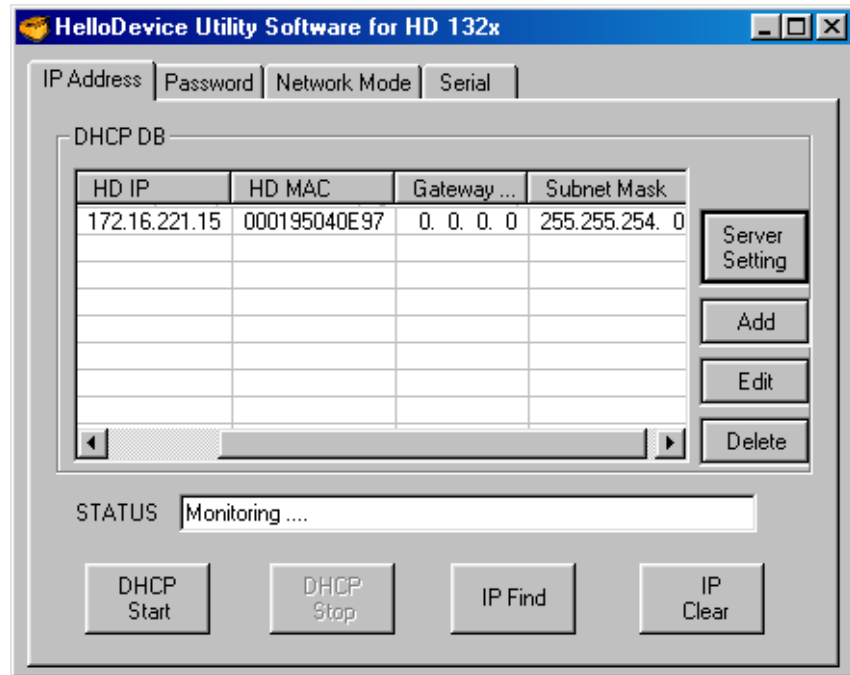
- 9 Enter the MAC address from the HD1320E (printed on the label) or KDE encoder, the IP address you wish to allocate (172.16.221.15 in this example) and subnet mask for LAN (255.255.254.0 here).



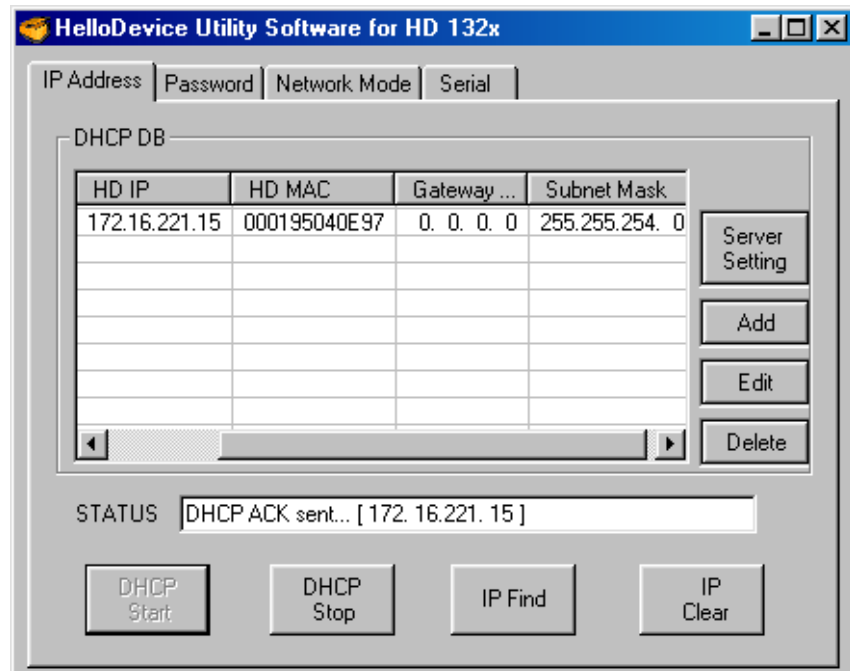
The 'DB Setting for DHCP' dialog box has a title bar with a close button. It contains several fields: 'MAC Type' with a dropdown set to '1', 'MAC Length' with a dropdown set to '6', 'IP' with a text field '172 . 16 . 221 . 15', 'MAC' with a text field '00 : 01 : 95 : 04 : 0E : 97', 'Gateway IP' with a text field containing three dots, 'Subnet Mask' with a text field '255 . 255 . 254 . 0', and 'Default Router' with a text field '172 . 16 . 221 . 41'. There is an 'Advanced..' button to the right of the 'Default Router' field. At the bottom are 'Add' and 'Cancel' buttons.

Click Add button.

- 10 Repeat step 9 for each connected HD1320E or KDE encoder you are setting up.

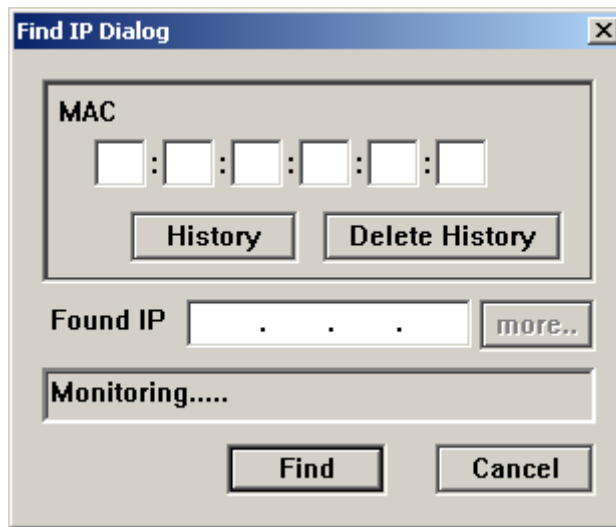


- 11 Power on the encoder(s) and the M200i(s). Press DHCP Start. Each encoder, identified in the DHCP DB table (by its MAC address) should now be allocated with the correct IP. Status messages similar to that shown should be received for each.



- 12 Press DHCP Stop.

- 13** Now, for each encoder, check that the IP address has been set as expected. Press IP Find, enter the encoder MAC address (or recall it using the History button) and press Find. The IP address should match that in the DHCP DB table on the main screen.



- 14** If any encoders have not had IP address set as expected it is either because there is another DHCP server present (see section on Physical Connection) or because they already had an IP address from a previous setup – see Changing an IP address below.

Changing an IP address

- 1** Make sure the configuration software DHCP server is not running. You can do this by checking the DHCP Start button is enabled.
- 2** For the encoder to be changed:
Press IP Clear, enter the correct MAC address (or recall it using the History button) and press Clear. Confirm when prompted.
The encoder now has IP address = 0.0.0.0 and will make a DHCP request. Press DHCP Start. The IP address from the DHCP DB table will now be allocated.

Setting TCP/IP port and COM parameters (Full Setup)

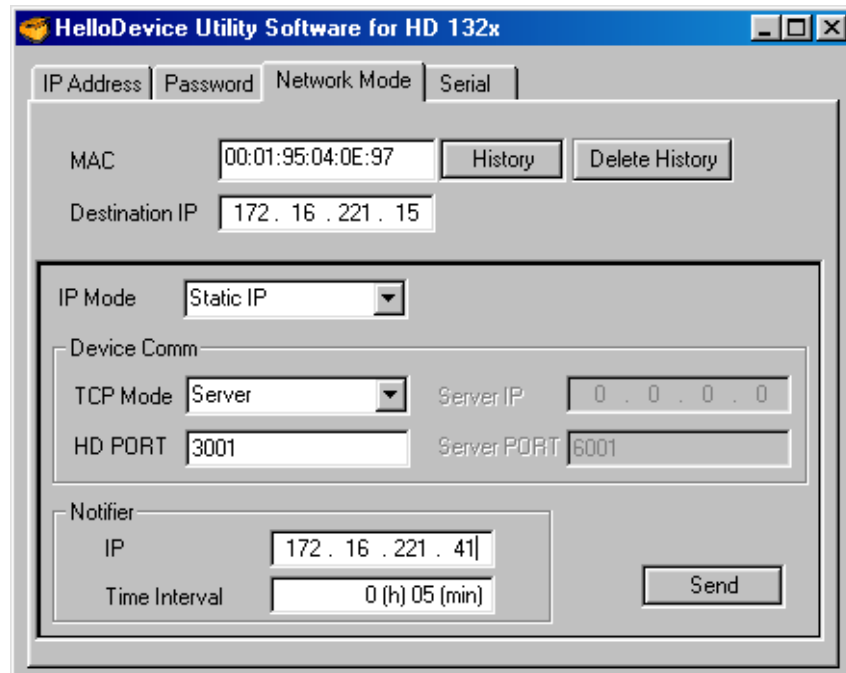
- 1 Click “Network Mode” tab. Type in MAC address or recall from history. Then select or type the parameters:

IP Mode: Static IP

TCP Mode: Server

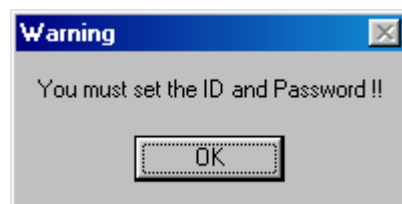
HD PORT: 3001

For “Notifier IP” type IP address of your PC (not important, as VingCard does not utilize it).

The screenshot shows the 'HelloDevice Utility Software for HD 132x' window with the 'Network Mode' tab selected. The window has four tabs: 'IP Address', 'Password', 'Network Mode', and 'Serial'. In the 'Network Mode' tab, the 'MAC' field contains '00:01:95:04:0E:97' with 'History' and 'Delete History' buttons next to it. The 'Destination IP' field contains '172 . 16 . 221 . 15'. Below these, the 'IP Mode' is set to 'Static IP' in a dropdown menu. Under the 'Device Comm' section, 'TCP Mode' is set to 'Server' in a dropdown menu, and 'HD PORT' is '3001'. To the right, 'Server IP' is '0 . 0 . 0 . 0' and 'Server PORT' is '6001'. Under the 'Notifier' section, the 'IP' field contains '172 . 16 . 221 . 41' and the 'Time Interval' is '0 (h) 05 (min)'. A 'Send' button is located at the bottom right of the form.

Then click Send.

- 2 Parameters set by “Network Mode” and “Serial” tab page are critical for proper operation of the serial server. So, the password is required to change them.

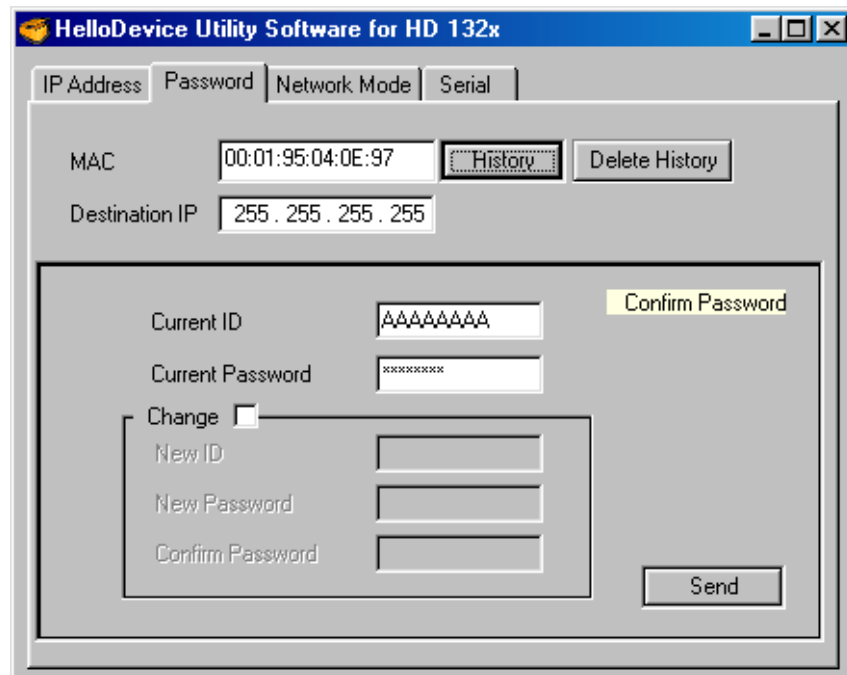


Click OK if you get warning. Then click on “Password” tab.

- 3 Type in MAC address or recall from history. Then type:

Current ID: AAAAAAAAAA

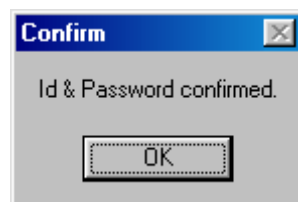
Current Password: AAAAAAAAAA (the asterisks will be displayed)



Advice: do not change ID's and passwords unless required by your LAN administrator.

Click Send to verify.

- 4 Wait for confirmation:



Now you can change network and com port parameters.

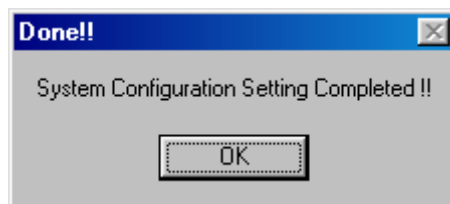
- 5 Click on Network Mode tab again

The screenshot shows the 'HelloDevice Utility Software for HD 132x' window with the 'Network Mode' tab selected. The window has four tabs: 'IP Address', 'Password', 'Network Mode', and 'Serial'. The 'Network Mode' tab contains the following fields and buttons:

- MAC: 00:01:95:04:0E:97 (with 'History' and 'Delete History' buttons)
- Destination IP: 172 . 16 . 221 . 15
- IP Mode: Static IP (dropdown menu)
- Device Comm section:
 - TCP Mode: Server (dropdown menu)
 - Server IP: 0 . 0 . 0 . 0
 - HD PORT: 3001
 - Server PORT: 6001
- Notifier section:
 - IP: 172 . 16 . 221 . 41
 - Time Interval: 0 (h) 05 (min)
- A 'Send' button is located at the bottom right of the form.

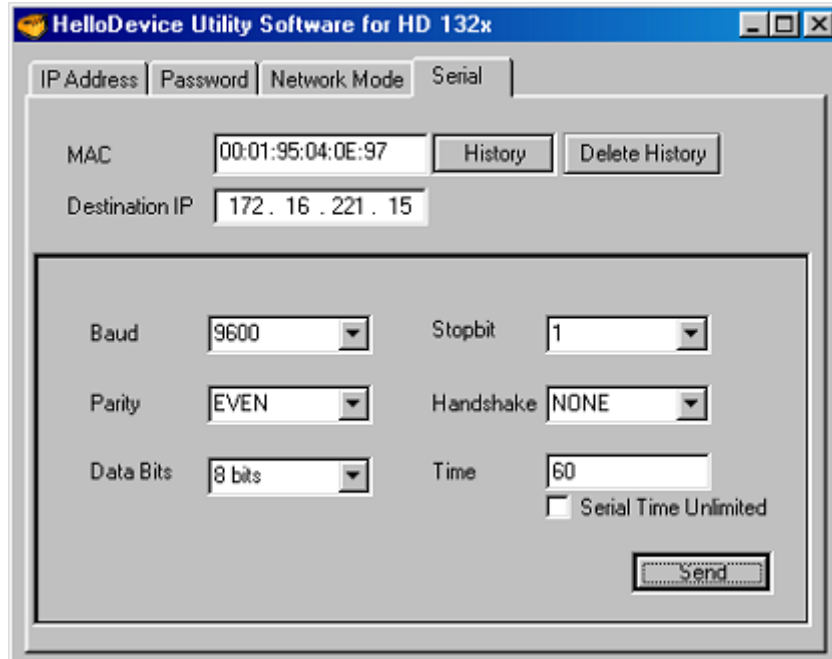
And check that all of the parameters are correct, then click Send.

- 6 Wait until HD1320E or KDE encoder confirms the change



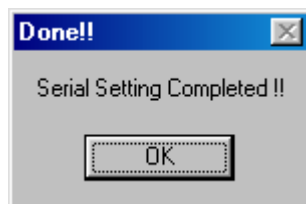
Click OK and select "Serial" page.

- 7 Type in MAC address or recall from history. Then select or type:
Baud: 9600
Parity: NONE (for KDE mag-card encoders) or EVEN (**different for P68 smart card encoders!**)
Data Bits: 8 bits
Stop Bit: 1
Handshake: NONE
Time: 60



Press Send button to update HD1320E or KDE encoder.

- 8 Wait for confirmation:



- 9 Repeat steps 1 to 8 for each connected encoder you are setting up.

Networking XAC Smart Card encoders

The XAC P68 Smart Card encoders that Vision utilizes are serial devices. If you want to connect them direct to the network you need to go through a serial server device (to convert data from the network to the correct serial format for the encoder).

Using Sena Technologies 'Hello Device'

The 'Hello Device' type HD1320E serial server is manufactured by Sena Technologies. This device allows Vision to address the encoder via an Ethernet network.



The Hello Device is the same device as held internal to the KDE network mag-card encoder (see earlier in this Chapter) and therefore Setup of IP address follows a similar procedure.

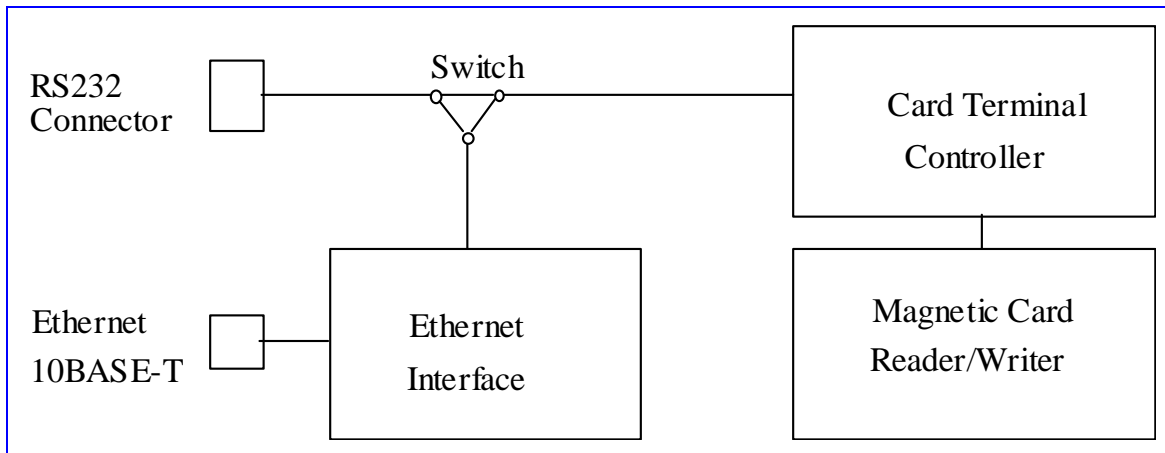
However, if HD1320E is purchased from another source than VingCard a.s in Norway - the serial settings are not exactly as per the KDE encoder, and you cannot use the custom set up program **SETUP4KDE.EXE**. You will need to use the full setup program **SETUP_HD132X.EXE** – see “Full setup Step by Step” section above. A complete manual for this version of the configuration software is available from www.sena.com . The XAC P68 requires the following serial configuration :

- 9600 baud,
- 8 bits,
- **EVEN parity**,
- no flow control
- time **must be** also set to 60 seconds.

Garek network encoders

Hardware Overview

Internal Block Diagram of Garek Network Encoder



NOTE: If the Card Terminal is used without Ethernet Interface, the switch connects the RS232 connector to the Card Terminal Controller. Otherwise, the switch connects the Ethernet Interface to the Card Terminal Controller. For configuration purposes, the Ethernet Interface can be switched to the RS232 connector.

Switch Positions

Overview of Garek Network Encoder Setup

Pos.	Connection	E.I. Mode	Remarks
1	EI ↔ Con	Configuration	Ethernet Interface configuration
2	CT ↔ EI	Configuration	Not applicable
3	none	Configuration	Not applicable
4	CT ↔ Con	Normal operation	via RS232
5	EI ↔ Con	Normal operation	Not applicable
6	CT ↔ EI	Normal operation	via Ethernet
7	none	Normal operation	Not applicable
8	CT ↔ Con	Configuration	Not applicable

Valid positions are **1**, **4** and **6**.

Garek Network Encoder Status LEDs

LED Color	Description
YELLOW	Power ON
GREEN	Signals card handling OFF - Card is not inserted. FLASHING - Waiting for card to be inserted. ON - Card is inserted.
RED	Signals errors OFF - Normal, no errors. FLASHING A FEW TIMES - a command did not succeed. FLASHING / LIGHTING LONG TIME - after power-up. EEPROM error. Try new power-up. If the error persists, service is needed.


How to Set Up (or change) the TCP/IP Address

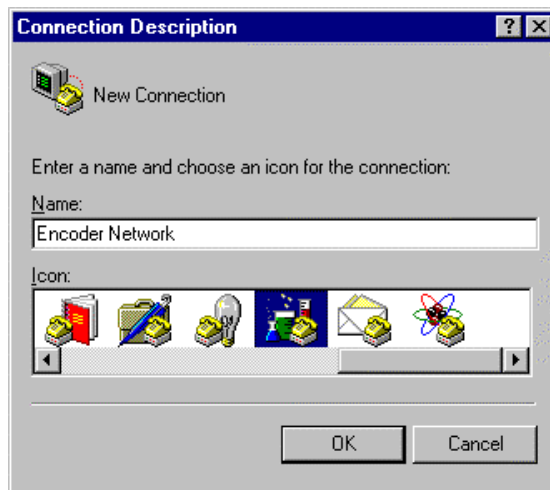
Hardware and Software Requirements

To set up the IP address you need to have a null-modem cable to connect the network encoder to a PC (or Vision workstation). You also need to have the **Hyperterminal** software, installed on all PC's running on Windows 95/98/NT/2000.

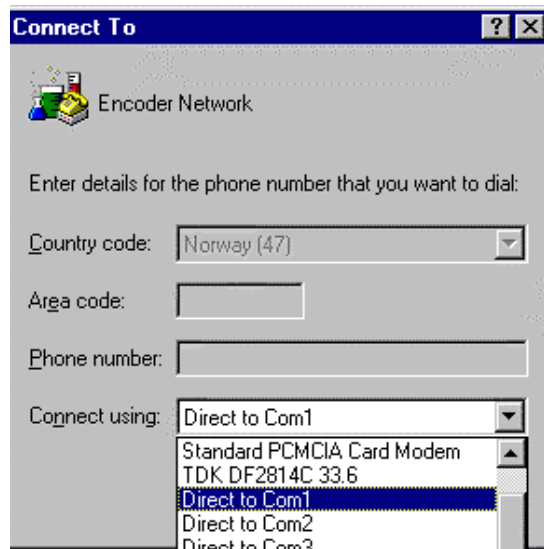
Models GA-MMW-1-N

In production until December 2000.

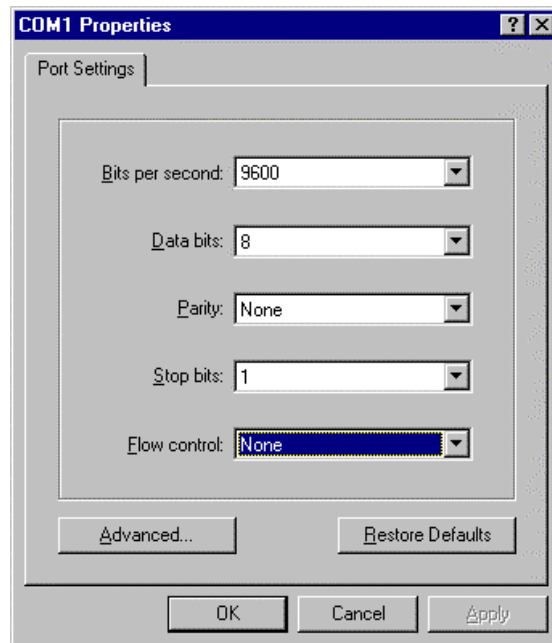
- 1 Click the Windows  button.
- 2 Click **Programs**.
- 3 Click **Accessories**.
- 4 Click **Communications**.
- 5 Double-click **HyperTerminal** and double-click on **HYPERTERM.EXE** to create a new connection.
- 6 Type a name for the connection and select one of the icons.



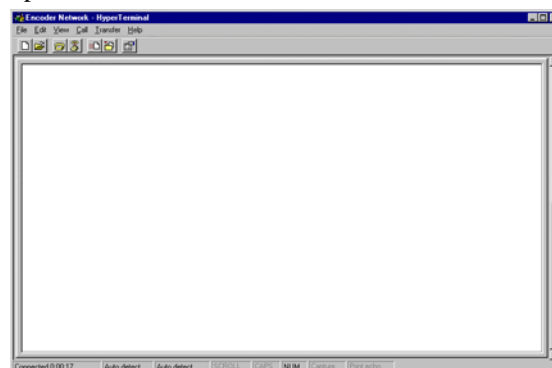
- 7 Click **OK**.



- 8 For **Connect using**, select **Direct to Com1** (or other serial port.)
- 9 Use the settings below for the COM port settings:



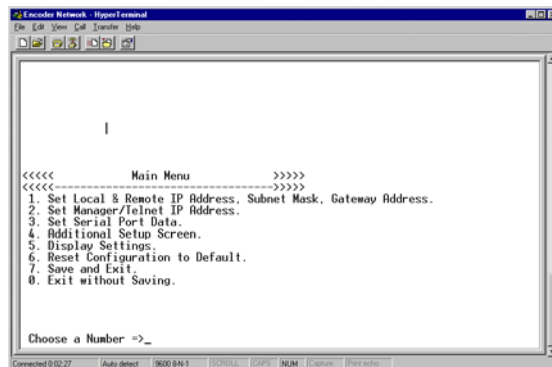
HyperTerminal is now ready to communicate with the network encoder to set up the TCP/IP address:



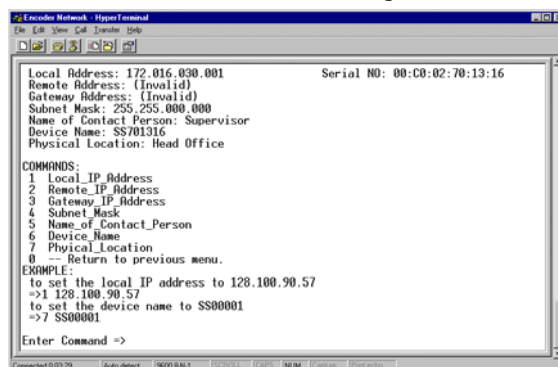
- 10 On the **Network Encoder**, set the switch to position **1**. Connect the serial

cable and plug in the power cord.

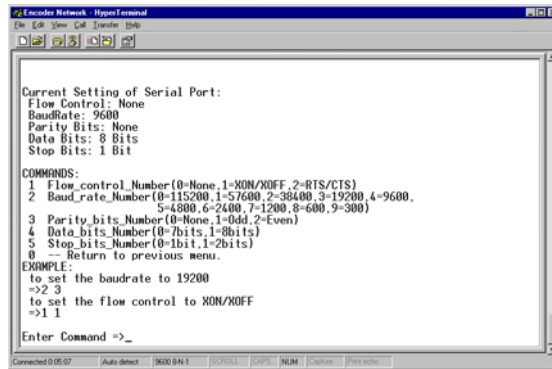
- 11 Wait a few seconds until the Serial Server Setup Program prompt is displayed on the screen. Press any key to access the Main Menu.



- 12 The following steps will assist you in modifying the following options:
Set Local & Remote IP Address, Subnet Mask, Gateway Address.
Set Serial Port Data.
Additional Setup Screen.
- 13 From the Main Menu type **1** (to set the IP and Subnet Mask.)
- 14 To modify the IP address, type the command **1 172.16.30.1** and press Enter. (The IP address must be unique on each unit.)



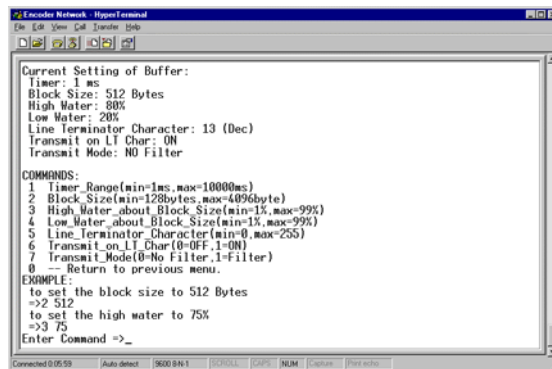
- 15 To modify the Subnet Mask, type the command **4 255.255.0.0** and press Enter. (The Subnet Mask is identical on all units.)
Type **0** to return to the Main Menu.
- 16 From the Main Menu type **3** to set Serial Port Data.
To set up the Flow_control_number to none type the command **1 0** and press Enter.
To set up the Baud_rate_number to 9600 type the command **2 4** and press Enter.



Type **0** to return to the Main Menu.

- 17** From the Main Menu, type 4 for the Additional Setup Screen.

To set up the Timer range, type the command **1 1** and press Enter.



Type **0** to return to the Main Menu.


- 18** The parameters are now set up. Exit from the Main Menu by selecting **7** (to save the new setting.)

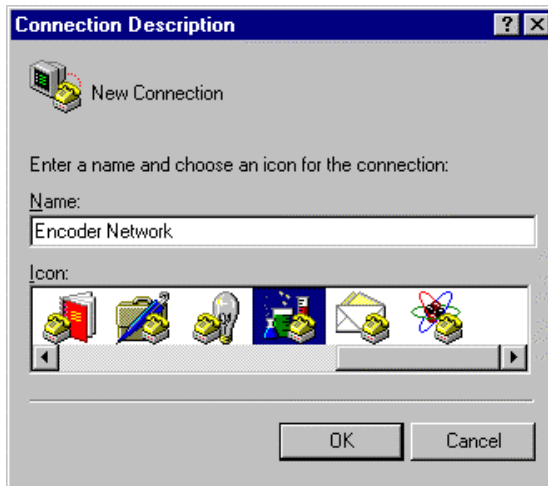
The encoder is now ready to be used on the LAN network.

NOTE: Before connecting the Network Encoder to the network, set the switch to position **6** for communication via Ethernet.

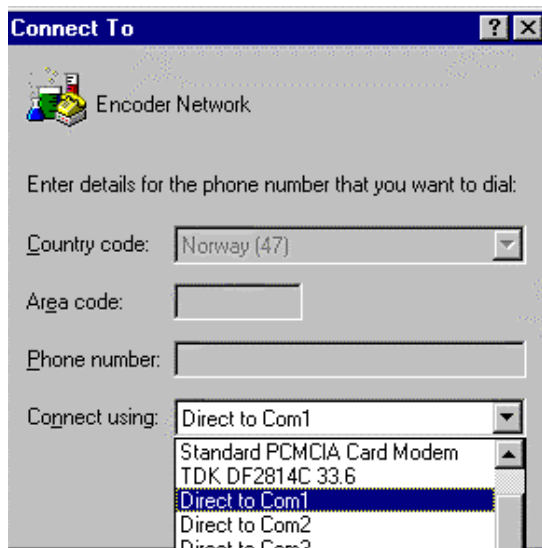
Models GA-MMW-1-NEM, GA-MMW-1-NXEM (wide track)

In production since December 2000.

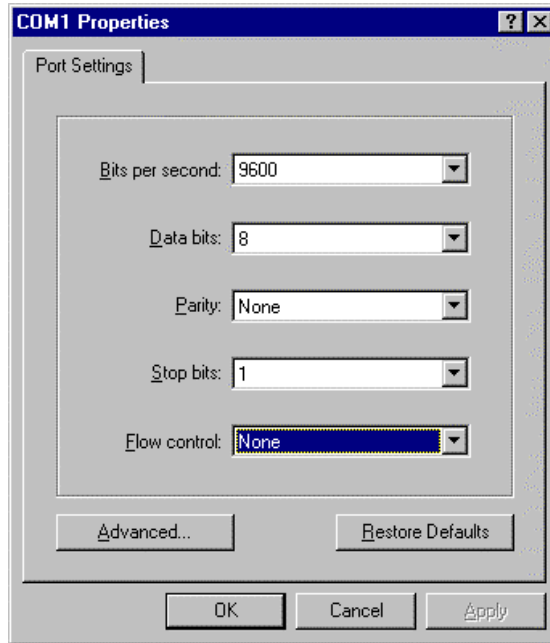
- 1 Click the Windows  button.
- 2 Click **Programs**.
- 3 Click **Accessories**.
- 4 Click **Communications**.
- 5 Double-click **HyperTerminal** and double-click on **HYPERTERM.EXE** to create a new connection.
- 6 Type a name for the connection and select one of the icons.



- 7 Click **OK**.

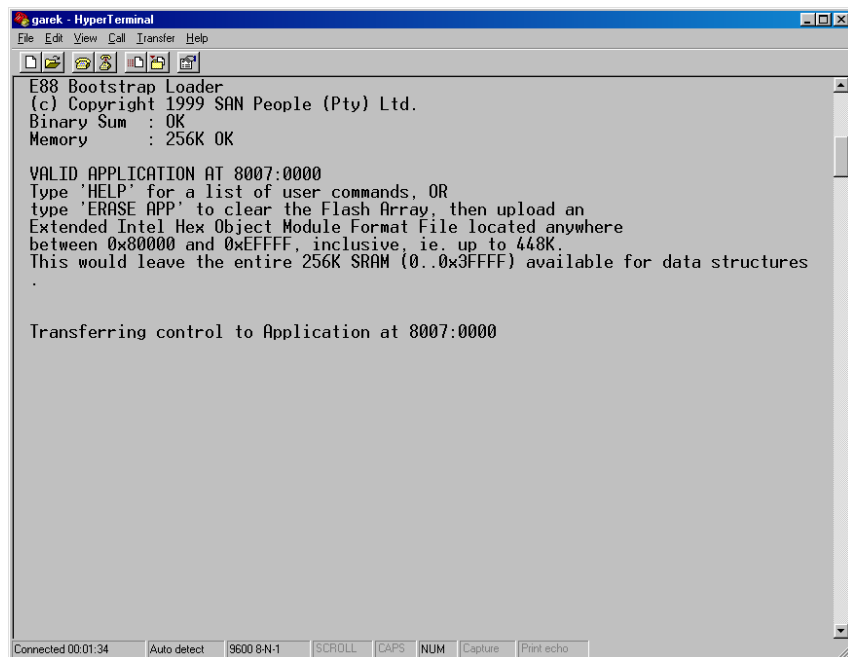


- 8 For **Connect using**, select **Direct to Com1** (or other serial port.)
- 9 Use the settings below for the COM port settings:

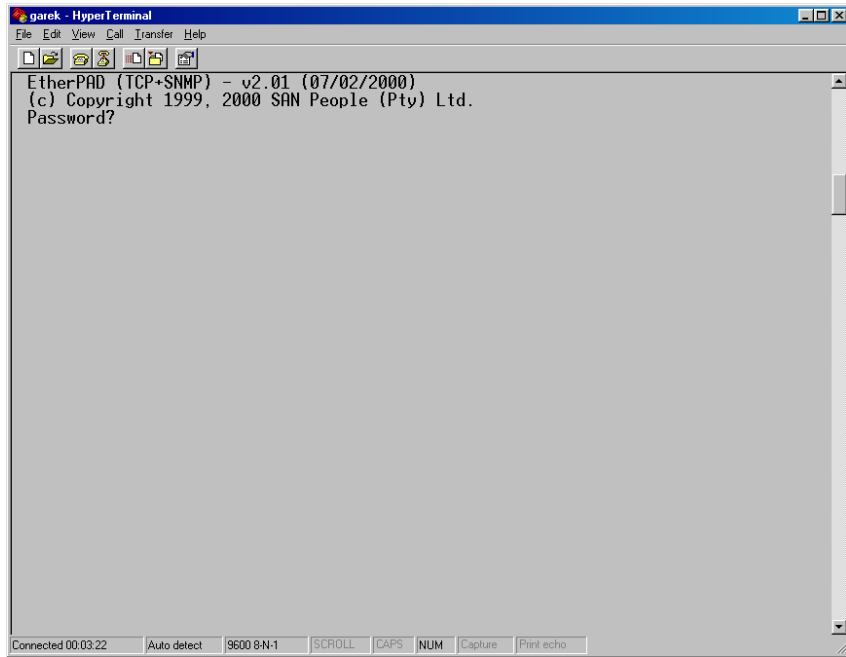


HyperTerminal is now ready to communicate with the network encoder to set up the TCP/IP address:

- 10 On the **Network Encoder**, set the switch to position **1**. Connect the serial cable, plug in the power cord and turn the switch on.
- 11 Wait a few seconds until the serial server boot text is displayed on the screen.

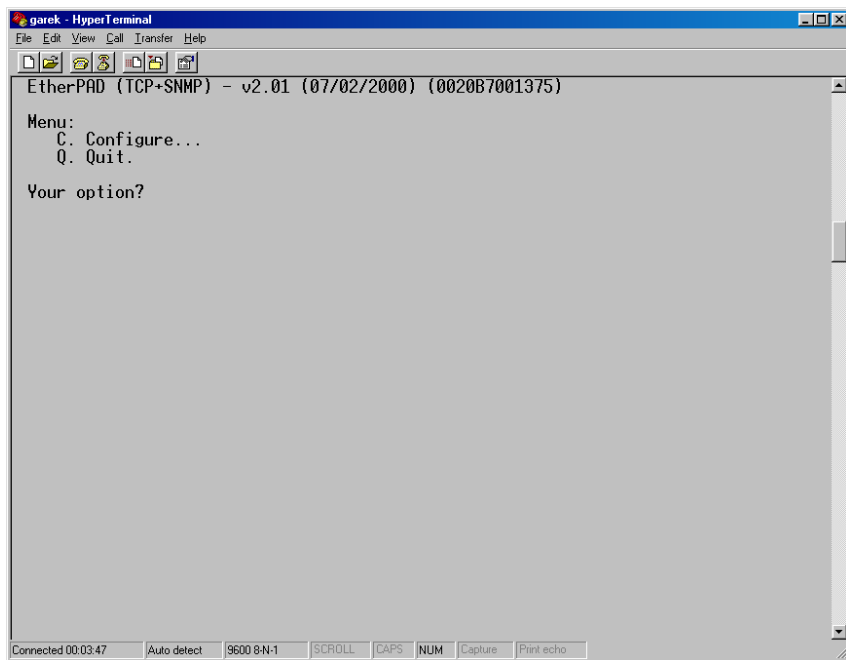


- 12 Wait more, until a prompt for password is displayed. Note that password entry has a timeout of 5 seconds only, so be quick.

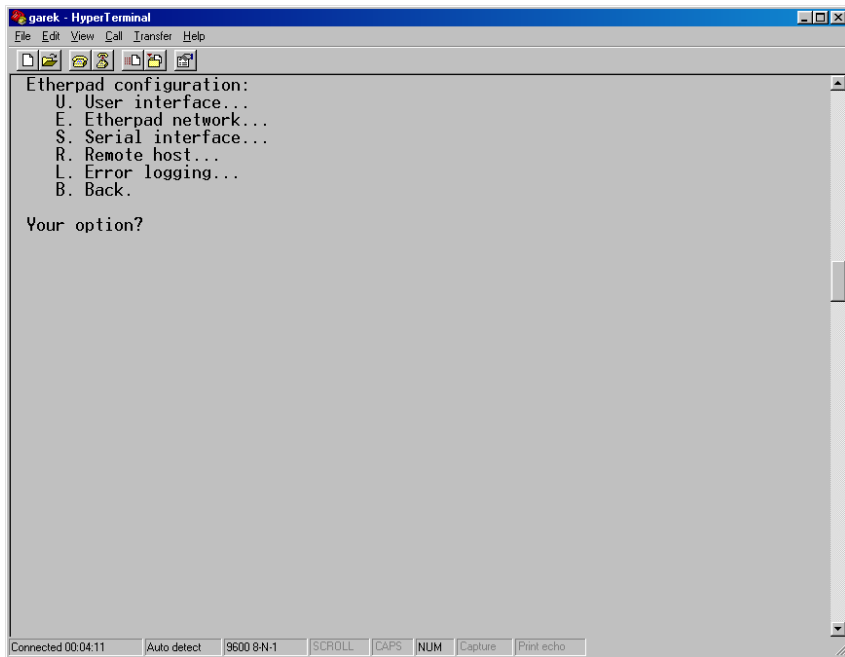


Type "xxx" as a password.

13 Main menu will be shown:

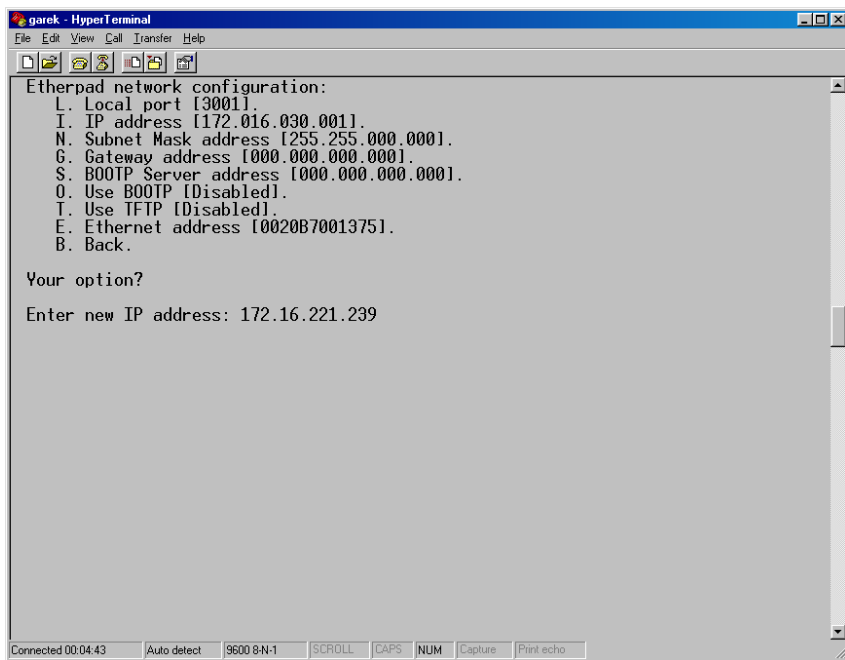


14 In the Main Menu type **C**, to configure serial server. You will see a configuration menu:



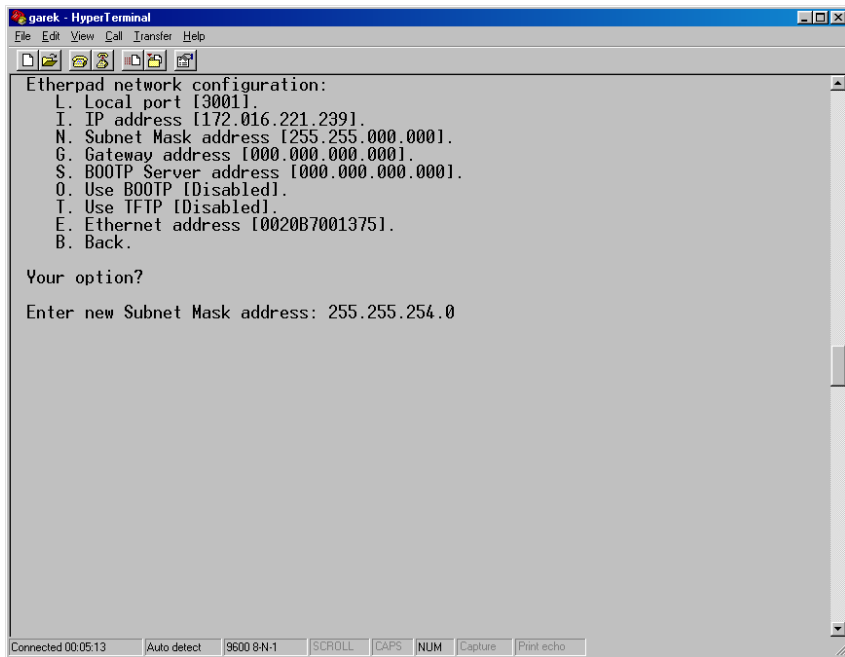
Type “E” for “Etherpad network“ configuration sub-menu.

15 Now you can modify the IP address and subnet mask



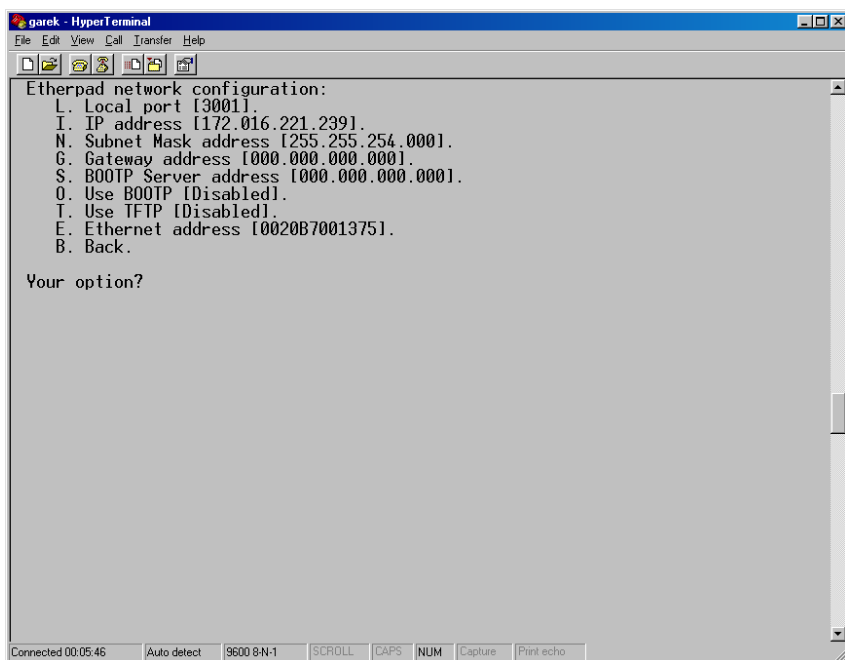
To modify IP address, type “I” and enter. Then type a new IP address (172.16.221.239 in this example).

16 To modify the subnet mask, type “N” and Enter.



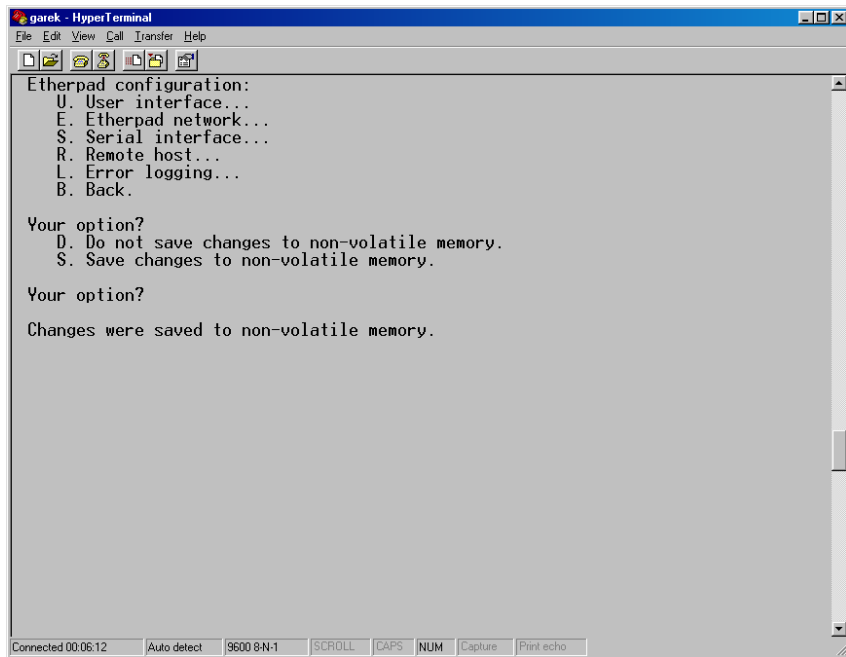
Then type a new subnet mask (255.255.254.0 in this example).

- 17 Check on screen, if the IP address and subnet mask are correct.



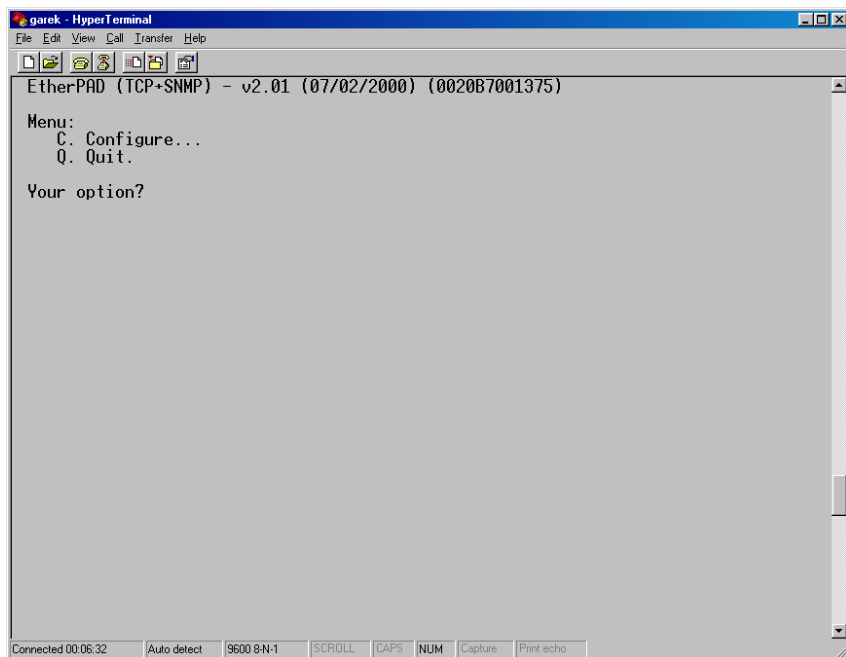
Then type “B” to go back to main menu.

- 18 You will be asked to save the changes.



Type “S” to save your settings in the unit.

19 The parameters are now set up.



Exit from the Main Menu by selecting “Q”.

The encoder is now ready to be used on the LAN network.

NOTE: Before connecting the Network Encoder to the network, set the switch to position **6** for communication via Ethernet.

Chapter 8 : Batch Mode

Introduction

This appendix describes how VingCard Vision operates in Batch Mode. This mode is designed to handle mass production of up to 3000 magnetic cards in one batch. Batch mode is primarily meant to handle passenger check-ins on ships, but could be used for other purposes as well.

Batch Mode is a variant of the standard VingCard Vision system. All functionality is the same with the exception of the PMS interface. In Batch Mode, check-in type commands from the PMS received via an RS232 or TCP/IP connection will not make keycards directly. Instead, they produce special data files containing keycard data in the queue folder. These files are regularly polled by external card printer software. When the printer software detects that the files are complete it uses the information in them to mass-produce keycards on a high volume card printer /encoder.

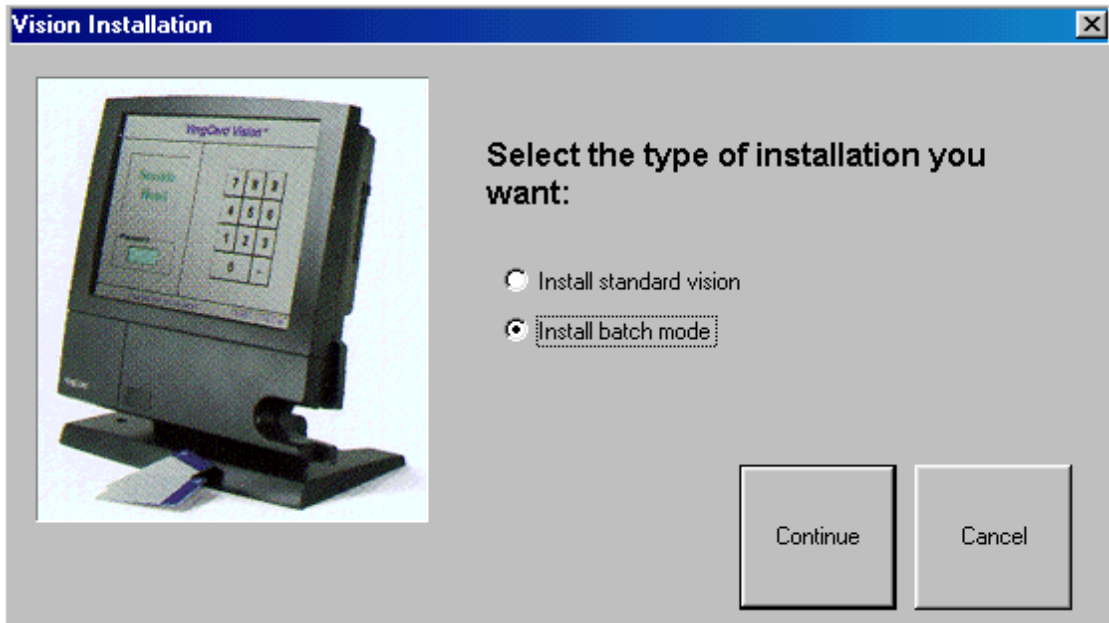
The magnetic card can be coded onto all 3 tracks and print information on the surface in one operation. A magnetic card printer and encoder must be used for this purpose. To produce about 2000 personal cabin keys with coded POS, key data, ID and name, dates and sailing information on the surface will take approximately 2 hours. The cards can be produced ahead of time (pre-issued) for a specific cruise. Normally the system should be located on the ship to handle upgrades, cabin changes and lost cards.

The magnetic card produced can be used for POS (Point of Sale), key to the cabin, gate entrance, passenger verification (ID card) etc.

The VingCard batch mode system needs to be connected to the ships/hotels PMS (Property Management System) to run the batch mode. The VingCard System will always be able to operate as stand-alone for key production.

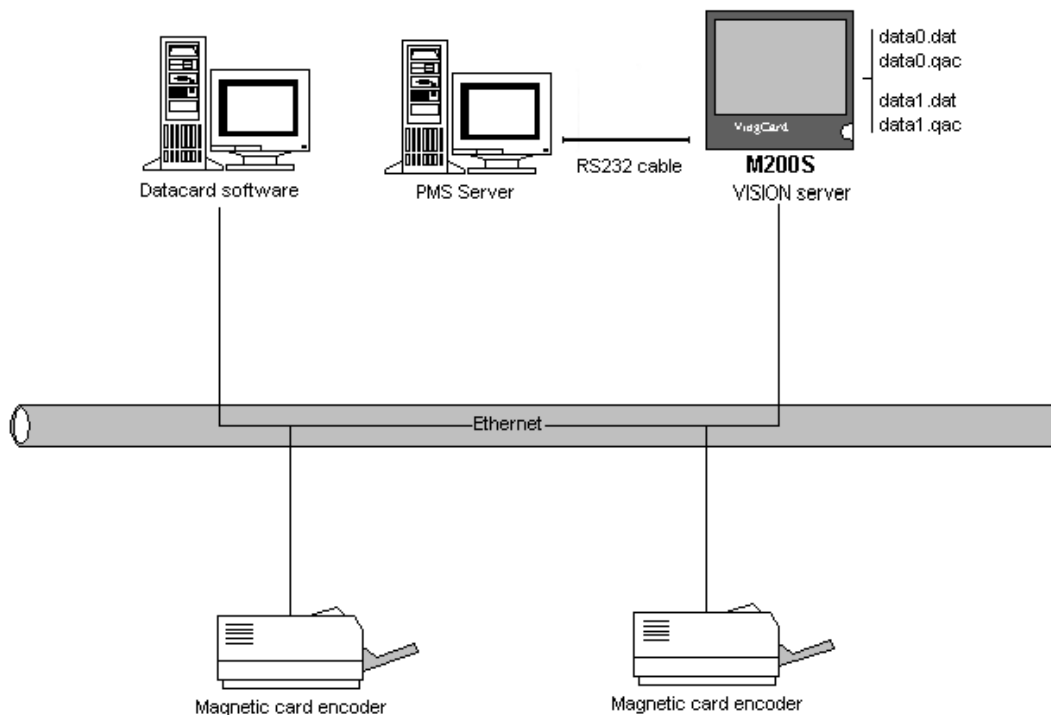
Installation

For general information about setup, installation and operation of the VingCard Vision keycard system, please refer to the chapters and appendices in this manual. When installing Batch Mode, the Batch Mode install option should be selected.



It is preferable that authorized VingCard personnel install the system. This manual is a guideline for them as well.

System Overview



PMS integration and interface

Vision and the PMS must be connected either via a RS232 cable connection or via Windows TCP/IP network. Please refer to Chapter 6 in this manual. The Vision station that is connected to the RS232 cable must run PMS.EXE in order for Batch Mode to work. Alternatively, if TCP/IP interface is selected, the Vision station must run VTCLINK.EXE. This can be set up via Setup – System Parameters – PMS RS232 or PMS TCP/IP.

Configuration File

Short text file MARINE.INI is placed in Vision folder during installation of the system. This file defines several parameters for processing a batch in Vision. Here is a content of it:

```
[Vision Marine]
Mode=batch
Format=Eltron
Path=C:\VISION\QUEUE
```

First parameter “Mode” must contain text “**batch**” (after equal sign) to turn the batch mode on. Anything else will put Vision into normal mode.

Second parameter “Format” can be set to either “**Eltron**” or to “**DataCard**”. If selected is “DataCard” then all fields in the output file will keep the same size – it means that Vision will fill up the remaining bytes with space character 0x20. If format is “Eltron” then fields will have variable size.

Last parameter “Path” determines the name of local or network directory, where an output file DATAnn.DAT and queue control file DATAnn.QAC are stored.

Communication

Communication PMS – Vision

The message format, control characters, commands and answer codes used with the Vision system in Batch mode are the same as those used in the standard version. The field usage is also mainly the same. Information about the above mentioned formats is found in Appendix A in this manual. The fields, which are used differently in Batch mode, are the Print information field and the Generic field.

The “Print information” field:

For the batch mode, the information in this field is printed onto the surface of the card. The field is 128 characters long, and is default divided into 4 fields. For example:

- Cruise Number // default 32 characters
- Ship Name // default 32 characters
- Sailing from // default 32 characters
- Sailing to // default 32 characters

The PMS must insert “spaces” to fill up the fields to 32 characters

The fields can be customized to meet the customer’s request. The customization must be done between VingCard and customer.

The “Generic” field:

In batch mode, the Generic Field is used to count down records to be received from PMS. If 1000 records shall be sent from PMS to VingCard, the first record will have the Generic Field = 1000, next 999 and so on. The last record will have the Generic Field = 1, which will cause handshake data to be written to the *.QAC file (which will until then have been empty).

Communication Vision - Magnetic card encoder

The communication between VingCard and printer software is done through a flat file transfer on a shared drive.

The file name will be "data0.dat" for printing to the magnetic encoder 0 (as defined in Vision- Setup – System Parameters – PMS RS232 – Address Mapping).

The file name will be "data1.dat" for printing to the magnetic encoder 1.

The file name will be "data2.dat" for printing to the magnetic encoder 2.

The file name "data0.qac" is handshaking file for data0.dat

The file name "data1.qac" is handshaking file for data1.dat

The file name "data2.qac" is handshaking file for data2.dat

Example:

Printer software polls all *.QAC files.

The file data.qac is 12 bytes long.

If the file is: 000000000000, means no action to be taken

If the file is: 000001000003, means print 3 cards, start with record 1.

If the file is: 000003000003, means print 1 card, start with record 3.

If the file is: 000001002000, means print 2000 cards, start with record 1.

As the printer software prints cards, it modifies the .qac file. When all cards have been printed, the file will read 0000000000.

Note that upon receipt of new commands from the PMS, VingCard Vision will only overwrite the .dat file associated with a specific encoder if the .qac file contains all zeroes – indicating that the printer software has produced all previously requested cards.

Operation of the Vision system in Batch mode

In Chapter 6 in this manual and in separate PMS interface manual, the interface protocol between PMS (Property Management System) and VingCard Vision is explained in detail. The protocol has a range of possibilities to fulfill almost every need.

Let us do an example:

The ship "DREAMBOAT" has 400 cabins. The ship will sail from New York to Miami on 4 July. It will arrive Miami on 11 July 2001. There will be 670 passengers on the voyage.

The PMS operator on the ship decides to run the batch on 2 July (pre issue). A check-in new command "G" must be sent for each check-in together with the required fields (see below).

Required fields for 1 passenger:

- Command G [*command code*]
- User Type PASSENGER
- Room Name (Cabin) 5010

- Family Name Smith
- First Name Jane
- Check in time 200107040600
- Check out time 200107132400
- User Group PASSENGER
- Track 1 ANYTHING
- Track 2 Point of sale #, ID etc.
- Print Info 123 ;cruise number
 Dreamboat ;ship name
 New York ;sailing from
 Miami ;sailing to
- Generic Field 670 ;number of record (next will
 be 669, then 668 and so on.
 When 1 is reached the card
 production will start.

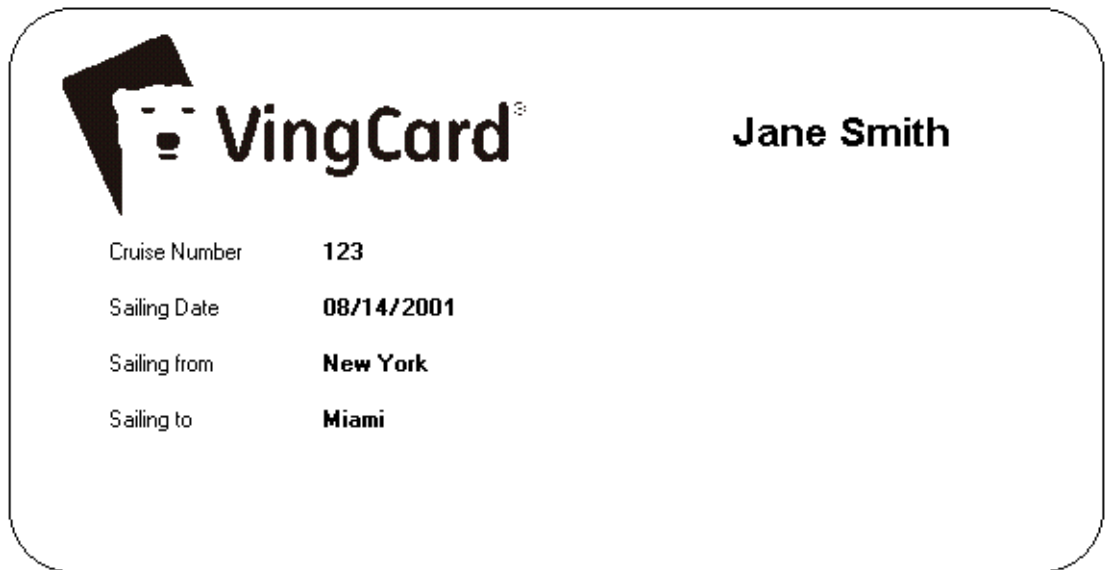
NOTE!

- The Print Info field is divided into 4 sub fields. Each field must be 32 characters long. Spaces shall be used as fillers.
- The check out date is extended by 2 days in case of arrival delay. A new passenger card will override the previous card anyway.
- The Generic Field is the batch activator. VingCard will wait until PMS have sent all records from 670 to 1. The 1 is the end batch for VingCard. VingCard will then send valid data to the QAC handshake file.

Keycards can be ordered with the logo and text of the user company's choice. This is an example of a card before encoding and printing:



This is the same card after encoding and printing:



An individual check-in must be sent for each passenger. An acknowledgement will be received by the PMS for every check-in. If a negative acknowledgement is received from VingCard, the check-in must be re-sent. One check-in command normally takes about 2 seconds.

When all the commands are received and acknowledged, VingCard will write valid data to the .qac handshake file. The card printer software will detect this handshake information and send all the data to the encoder for card production. One card takes about 4 seconds for this operation. Time required to produce 670 cards is: 670 cards x 2 seconds x 4 seconds = 5360 seconds = 1,5 hours. The batch should be run off peak time.

Producing / modifying single cards in batch mode

After a batch is run and the passengers have received their personal cards, the request for cabin change, name changes, lost cards, etc., will occur. In this case single cards must be produced.

The single card is produced in exactly the same way as the batch mode. It is a batch mode encoding and printing producing one card only.

To do this, enter 1 in the “Generic Field” field. This 1 means that this is the last record in the batch, and production will start.

Batch Mode File Formats

For each card stored in the DAT file the format is as follows.

If a full field size is not required, a CR-LF pair terminates each field after the text.

However, in some circumstances it may be necessary to pad each field to its full length using “space” character (ASCII character 0x20). To do enable this fixed record size (all fields padded by spaces) add the line “Format=DataCard” in the MARINE.INI file (main Vision folder). CR-LF pair terminates each field.

Example:

Maximum Field size. With “DataCard” format all fields will be set to maximum size by adding 0x20 character

	// 35 ASCII char Track 3 (Reserved for VingCard)
07/03/2003	// 32 ASCII char Sailing Date
07/10/2003	// 32 ASCII char End Date
12345	// 32 ASCII char Cabin
ABCDEFGH1234567890	// 79 ASCII char Track 1
1234567890	// 39 ASCII char Track 2
Jane Smith	// 64 ASCII char Passenger Name
123	// 32 ASCII char Cruise Number
Dreamboat	// 32 ASCII char Ships Name
New York	// 32 ASCII char Sailing From
Miami	// 32 ASCII char Sailing To

Chapter 9 : Import Export

Introduction

The Export database and Import database programs makes it possible to export and import databases to allow rapid check-in for multiple guests for whom keys have already been made and whose details are stored in a “source” database separate to the main Vision database. The functionality of the two programs is basically the same: They move data form a source database a destination database. Upon running Export database, data is exported from a local ‘source’ database to a remote ‘destination’ database. Upon running Import database, data is imported from a remote ‘source’ database to a local ‘destination’ database. The result is the same: When either of the programs is used, all data about guests (with the selected keycard types) in the main Vision database (the destination database) will be replaced by data form the source database.

This operation is useful in installations such as cruise liners, as it means that keys and database records can be prepared for the next cruise to be processed while the current cruise is still in operation. The new records can then be imported to the main (“current”) database at an appropriate time.

Export database and Import database are available on the Start Menu - Programs - VingCard – Vision.

General Information

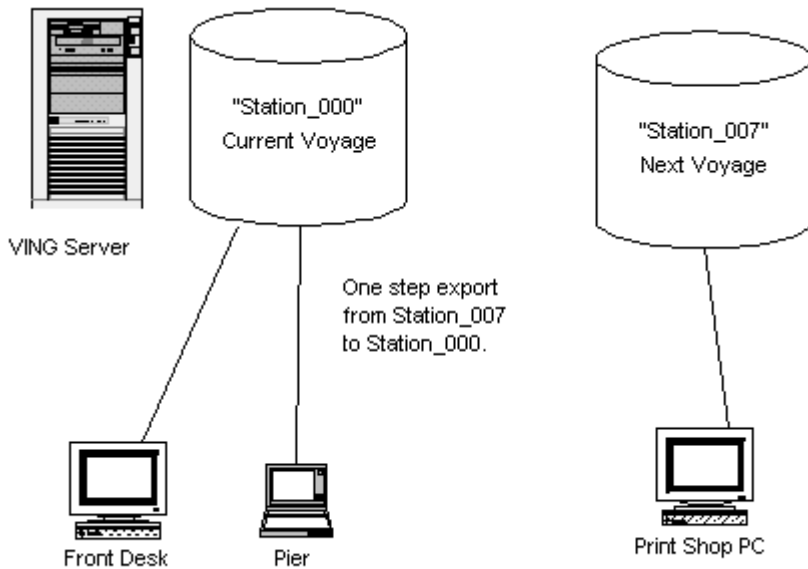
The Exporter and Importer programs move guests of the selected types from the source database to the destination database. Both the source and destination databases must be loaded and running on a database server. The databases are selected via the two drop-down list boxes. The names presented in the list boxes refer to ODBC system data source names (DSNs). The workstation that is running EXPORTER or IMPORTER must be set up with an appropriate ODBC system data source name (DSN) for both the source and destination database. These ODBC sources are configured with the database type, and one or more of the database file path, server name and database name assigned by the server. A DSN allows programs to locate and access specific databases. Three DSNs are provided when installing Vision. These are:

VINGCARD_SQL (which gives access to the main Vision database for the Hotel or Cruise Liner);

SOURCE_DB which searches all network drives for a database named Source, running on a SYBASE ASA type server also named Source.

DEST_DB which searches all network drives for a database named Dest running on a SYBASE ASA type server also named Dest

Visual representation of how the Import/Export process works



Moving guests to the main Vision database

This is an example of the export process based on the above diagram. The import process will be the same, except from that the Import database program is run from STATION_000 and imports the database from STATION_007.

Ensure that the Vision database server is running on STATION_000. (If you can run Vision and access a list of rooms in the Guest keycard module, the database server is running). If the database is not running, it can be started from the Start menu – Programs – VingCard – Vision – Vision ASA Server..

Run a database server on STATION_007. This can be started from Start Menu - Programs - VingCard - Vision - Generic ASA Server. In the ASA Server startup dialog, set "Database" to the appropriate .DB file (the one that the guests will be exported FROM) and Server Name to "Source".

Start Exporter on STATION_007. (Start Menu - Programs - VingCard - Vision – Export Database).

Select SOURCE_DB as the source database, VINGCARD_SQL (which is the main Vision database) as the destination

Select the guest user groups (keycard types) you want to import.

Press Export. This exports the guests registered with the selected user groups into the main Vision database.

NOTE: Failure to perform the Import or Export function prior to a voyage will result in using an outdated database for that voyage.
THE IMPORT PROCEDURE MUST BE RIGOROUSLY FOLLOWED.

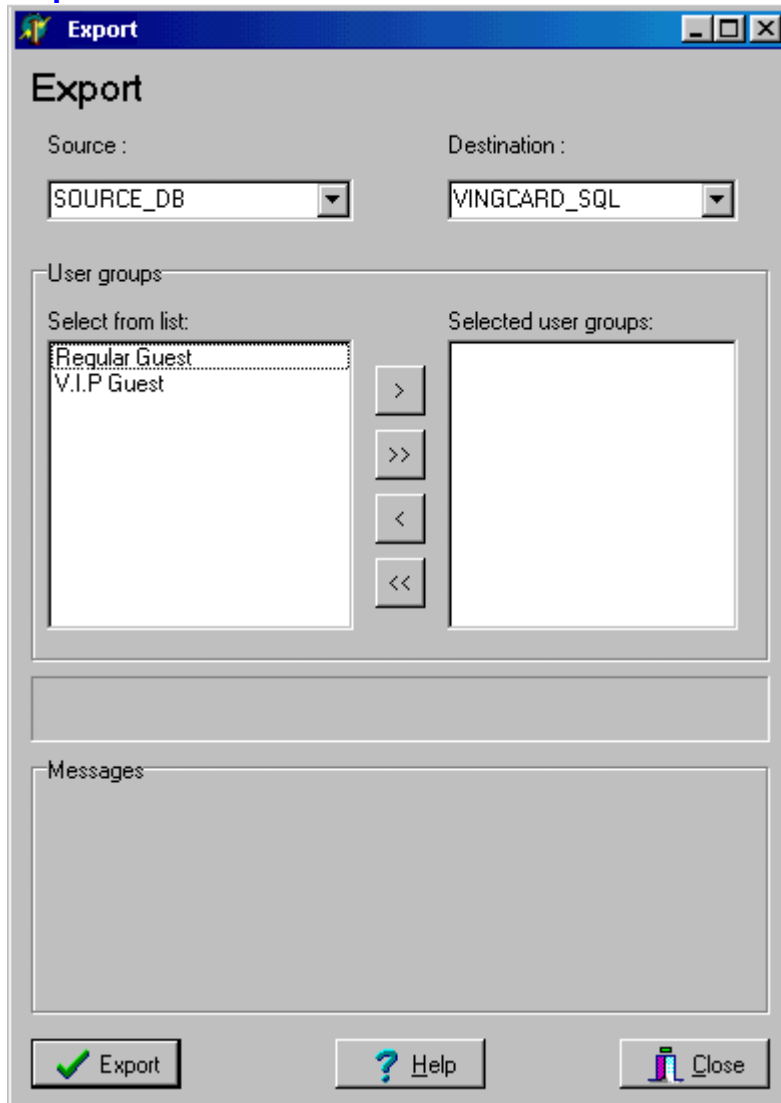


WARNING! After an Import or Export function has finished (when the new guest database has been successfully moved to the main Vision database), the source database will be empty for the User groups which were imported. The destination database will be updated with the data removed from the source database. Since the source database no longer holds the guest information, the import or export process can only be performed ONCE from one database. Remember to ALWAYS take a backup of the remote (to be imported or exported) database before starting the process.

The Import Screen

Option	Description
Source	Select the database you are importing from, in this case the source database is called "SOURCE_DB".
Destination	Select the main Vision database, VINGCARD_SQL (the database you are importing into).
User groups	Select one or more of the entries in the "Select from list" section. Move the selected entries to the "Selected user groups" section by clicking the move buttons between the sections..
Messages	Messages concerning the import process are shown here.
Import	Click this button to start the import process when you are done making changes to the screen.
Help	Click this button to view the on-screen help for the import process.
Close	Click this button to close the Importer program.

The Export Screen



Option	Description
Source	Select the database you are exporting from, in this case the source database is called "SOURCE_DB".
Destination	Select the main Vision database, VINGCARD_SQL (the database you are exporting to).
User groups	Select one or more of the entries in the "Select from list" section. Move the selected entries to the "Selected user groups" section by clicking the move buttons between the sections..
Messages	Messages about the import process will be shown here.
Export	Click this button to start the export process when you are done making changes to the screen.
Help	Click this button to view the on-screen help for the export process.
Close	Click this button to close the Exporter program.

Chapter 10 : Using NBS Encoders

Introduction

This chapter describes the use of card encoder /printers manufactured by NBS
www.nbstech.com

Vision has the ability to interface to NBS encoder / printers such as the ImageMaster and ImageAce. This involves Vision issuing a specially formatted message that includes both encoding information (for the card magnetic stripe) and print information (for the card face). This message format and the protocol used to send it are different from the standard Vision encoder interface, therefore Vision setup contains an option that enables card encoding to be carried out on NBS encoder / printers.

This appendix includes

- How to set up Vision to communicate with NBS encoders
- An example of how to set up an NBS ImageMaster encoder to print and encode the information it receives from Vision

How to set up a Vision system to use NBS Encoders

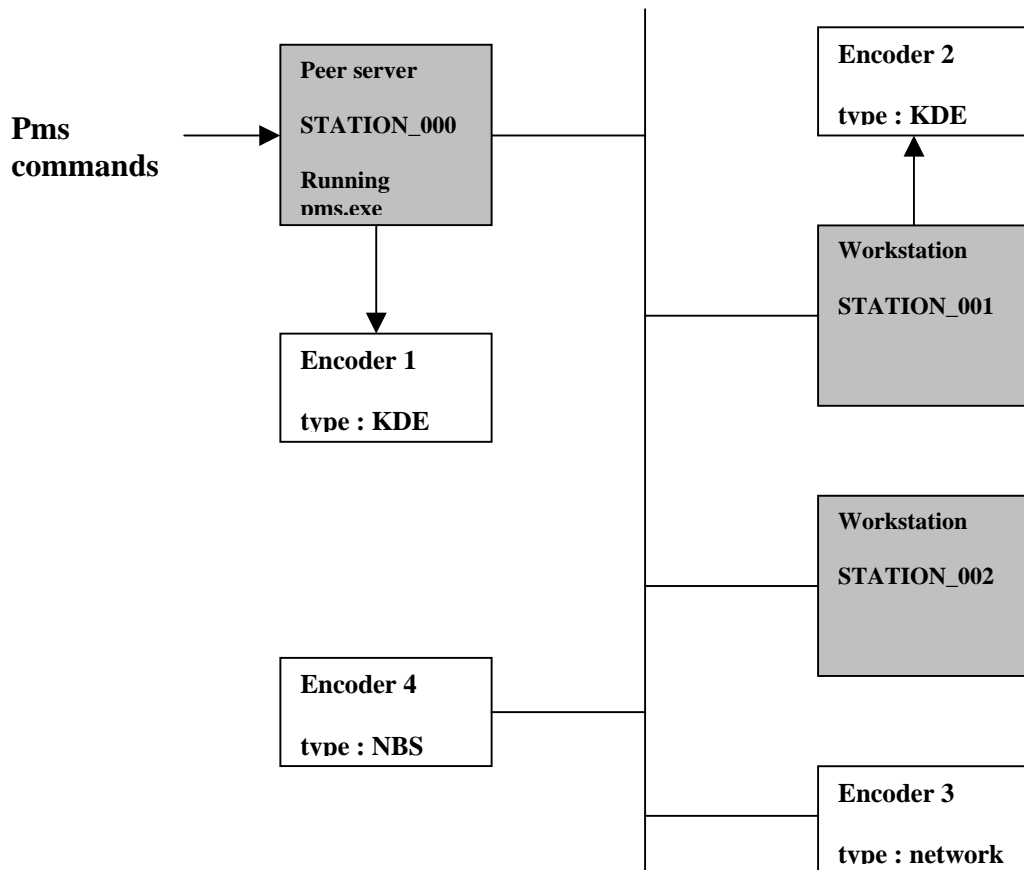
The NBS Encoder option (**Setup - System Parameters -General**) only affects card encoding that is:

- Triggered by a PMS command received via the RS232 link
- AND
- Is sent by the PMS to an address that maps directly to an Encoder defined in the M200i table (Setup - System Parameters –M200i)

Card encoding triggered in any other way (for example, from the workstation screen or by the PMS TCP/IP method) will be unaffected and will work in the usual manner using the standard Vision -> encoder interface and protocol.

It is possible to set up a Vision installation that can encode both on standard encoder types and NBS encoders. Consider the following example:

Example Vision Network supporting KDE, network and NBS Encoders :



Configuration in setup module:

M200I table <i>M200I tab</i>		
name	IP address	port
Encoder 3	xxx.xx.xx.xx	yyyy
Encoder 4	xxx.xx.xx.xx	yyyy

PMS Address Mapping <i>PMS RS232 tab, Address Mapping</i>	
PMS address	Encodes on
00	STATION_000
01	STATION_001
02	STATION_002
03	Encoder 4

Encoder mapping <i>Encoder tab</i>	
STATION_000	local
STATION_001	local
STATION_002	M200I, Encoder 3

In this example, and with the NBS Encoder option checked, it is possible to make cards on all Encoders from the PMS RS232 link. Because the NBS Encoder, Encoder 4 is mapped directly from the 'PMS Address Mapping' table to the 'M200I table' it receives its commands in NBS format.

Note that if the 'normal' Network Encoder, Encoder 3 was mapped directly to a PMS address, rather than indirectly, via STATION_002 as shown, then commands would be sent to it in 'NBS format' and encoding would not occur.

How to set up NBS Encoders for use with Vision

This section gives an example of how to set up an NBS ImageAce encoder to both encode and print the card information sent from Vision.

For full and up to date information on NBS products and procedures, use www.nbstech.com

Information sent from Vision to NBS

The information sent via TCPIP from Vision begins with an STX character, ends with an ETX character and in between contains 14 fields, each separated with a Carriage Return character. The 14 fields are as follows

field	comment
Guest Name	Combined First & Family Name as received by Vision from the PMS
Check In Date	As received by Vision from the PMS
Check Out Date	As received by Vision from the PMS
Variable 1	16 characters. Part of the print information field received from the PMS
Variable 2	16 characters. Part of the print information field received from the PMS
Variable 3	16 characters. Part of the print information field received from the PMS
Variable 4	16 characters. Part of the print information field received from the PMS
Variable 5	16 characters. Part of the print information field received from the PMS
Variable 6	16 characters. Part of the print information field received from the PMS
Variable 7	16 characters. Part of the print information field received from the PMS
Variable 8	16 characters. Part of the print information field received from the PMS
Track 1 Data	For encoding on track 1 as received by Vision from the PMS, field '1' ISO IATA specification (excluding start & end sentinel)
Track 2 Data	For encoding on track 2 as received by Vision from the PMS, field '2' ISO ABA specification (excluding start & end sentinel)
Track 3 Data	For encoding on track 3 – this is the VingCard key data VingCard encrypted format

Table 1: Data fields from Vision to NBS

Fields variable 1 – 8 are derived from the Print Information field as sent from PMS to Vision using the 'I' data field. The total length (128 characters) of the 'I' field is split into 8 x 16 character fields, giving maximum flexibility in the data that can be sent by the PMS for formatting and printing onto the cards.

It is important that the PMS vendor correctly pads out each of the 8 sub-fields that is used to be the correct length (16 characters). Unused fields can be left off. Example : to send 2 sub-fields, 'Apple' and 'Orange' the PMS 'I' data would be

A	p	p	l	e											
O	r	a	n	g	e										

each empty box represents a space character.

Vision chops the PMS 'I' data into 16 character chunks and appends a carriage return character to each before sending the data on to the NBS encoder.

Setting up NBS to use the information

Having received the above data, the NBS encoder / printer can be set up to print as much of the information as it wants to onto the card and also to encode the card. To do this, the NBS equipment must be set up with the required field, font and position information.

The following is an example of how to do this for the NBS ImageMaster / Ace. In this example, all three encoder tracks are encoded and seven of the fields sent by Vision are printed : Guest Name, Check In Date, and the first five of the 16 character variable data fields, in this case designated

data field	name
1	GRP
2	FOL
3	VIP
4	Adult
5	Child

(The other 3 variable fields are not used).

Machine Settings setup

Enter UTILITY > SYSTEM > MONITOR menu and type "E 6000:110"<RET>. Then enter "01" <RET>. This selects the DUALCO encoding board option. Press [ESC] 3 times to return to main menu.

Enter UTILITY > COMM > HOST > SETUP menu and change baud rate to 9600 (to match Vision). Press [ESC] 3 times to return to main menu.

Enter UTILITY > SYSTEM > MACHINE > ENCODE > TRACK 3 > SETUP menu and change the bits per char value to 0. This selects the VingCard encoding format for track 3. Press [ESC] 3 times to return to main menu.

Layout Creation

This example assumes that the following information is represented in the variable fields

Enter UTILITY > LAYOUT > CREATE menu and enter the layout name "GSTCARD"
Create a LAYOUT called GSTCARD and then edit the layout
Press [SHIFT]&[INS] 24 times to create 24 default fields.

1	x=0.01 y=0.01 Transfer=Source on Source ID=GRP Accept=Host
2	x=0.02 y=0.02 Transfer=Source on Source ID=CKOT Accept=Host
3	x=0.03 y=0.03 Transfer=Source on Source ID=CKIN Accept=Host
4	x=0.04 y=0.04 Transfer=Source on Source ID=NAME Accept=Host
5	x=0.01 y=0.08 Transfer=Source on Source ID=FOL Accept=Host
6	x=0.01 y=0.07 Transfer=Source on Source ID=VIP Accept=Host
7	x=0.01 y=0.06 Transfer=Source on Source ID=ADLT Accept=Host
8	x=0.01 y=0.05 Transfer=Source on Source ID=CHLD Accept=Host
9	Accept=Host
10	Accept=Host
11	Accept=Host
12	Type=Encode Name=IATA Accept=Host Maxchars=69
13	Type=Encode Name=ABA Accept=Host Maxchars=39
14	Type=Encode Name=MINTS Accept=Host Maxchars=103
15	Fontname=DCH140B x=1.70 y=1.80 Justify from=Center Transfer=Dest on Dest ID=NAME Strip spaces=Yes
16	Fontname=DCH100B x=3.04 y=0.45 Justify from=Right Transfer=Dest on Dest ID=CKOT Strip spaces=Yes
17	Fontname=DCH100B x=0.60 y=0.80 Transfer=Off Accept=Fixed
18	Fontname=DCH120B x=1.70 y=1.95 Justify from=Center Transfer=Dest on Dest ID=GRP Strip spaces=Yes
19	Fontname=DCH080B x=3.04 y=0.30 Justify from=Right Transfer=Dest on Dest ID=FOL Strip spaces=Yes
20	Fontname=DCH100B x=3.04 y=0.60 Justify from=Right Transfer=Dest on Dest ID=VIP Strip spaces=Yes
21	Fontname=DCH080B x=2.40 y=0.30 Transfer=Off Accept=Fixed Fixed Text=No:
22	Fontname=DCH080B x=2.95 y=2.05 Transfer=Dest on Dest ID=ADLT Strip Spaces=Yes
23	Fontname=DCH080B x=3.04 y=2.05 Transfer=Dest on Dest ID=CHLD Strip Spaces=Yes
24	Fontname=DCH080B x=3.00 y=2.05 Transfer=Off Accept=Fixed Fixed Text=/ /

1000

Press [ESC] to exit layout editor
Press 'Y' to save layout
Press [ESC] 3 times to return to main menu.
Select "Layout" from the main menu and press <ENTER>
Select the CHECKIN layout
Select "Print" from the main menu and press <ENTER>

The Unit is now ready to accept data for card production.

Notes on Field order

Note that Vision sends the data, via TCPIP in the order shown in table 1 but that the NBS equipment is set up in a different order with field Variable 1 (in the example, labeled GRP) first etc. See table 2 for an example.

Power Down & Reset

Note that following power down or reset of the NBS machine, you must select "Print" and press <ENTER> from the main menu in order to put the machine online. The message "WAITING FOT HOST DATA" will appear on the LCD screen when the NBS is ready. If the unit is set into any other mode by mistake, either a command mode or an HP LaserJet emulation mode, it can be returned to normal operation by simply pressing RESET, then press [ENTER]. "WAITING FOR HOST DATA" will then appear.

If a card becomes stuck or jammed in the unit, the unit can be flushed by selecting:

[UTILITY] -> [SYSTEM] -> [TEST] -> [FLUSH]*

*Note that flush is not immediately displayed on the [TEST] menu. The cursor must be moved off of the screen to the right to display this option.

Resetting machine settings

To reinitialize the machine setup, open the back cover and turn DipSwitch #1 on. Turn power ON and you will be prompted to turn DipSwitch #1 off. When you do this, the default machine setup will be reloaded. Please refer to the above information to re-enter the required machine settings. The layout will remain intact.

Saving and Restoring a backup of the layout

To backup the layout "GSTCARD" into "GSTBAK"

Push RESET
Select [Utility] -> [LAYOUT] -> [COPY]
Select [GSTCARD]
Type GSTBAK [ENTER]
Push [ESC] [ESC] to return to main menu

If catastrophic changes are made to GSTCARD, the layout can be restored by copying the layout "GSTBAK into a new layout "GSTCD2."

Push RESET
Select [Utility] -> [LAYOUT] -> [COPY]
Select [GSTBAK]
Type GSTCD2 [ENTER]
Push [ESC] [ESC] to return to main menu
Select [LAYOUT]
Select [GSTCD2]

Push RESET
Push [ENTER]

